A comprehensive approach to support the external auditor of the small and medium audit firm, to address evolving information technology control risks of an auditee

by
Mrs Natasha Sexton

Thesis presented in partial fulfilment of the requirements for the degree Master of Commerce (Computer Auditing) at Stellenbosch University

Supervisor: Prof. Riaan Rudman
Faculty of Economic and Management Sciences

March 2017

Declaration

By submitting this thesis electronically, I declare that the entirety of the work contained therein is my own original work, that I am the sole author thereof (save to the extent explicitly otherwise stated), that reproduction and publication thereof by Stellenbosch University will not infringe any third party rights and that I have not previously in its entirety or in part submitted it for obtaining any qualification.

Date: March 2017

ACKNOWLEDGEMENTS

I would like to express my deepest gratitude to my friend Professor Riaan Rudman for the support, comments and engagement through the learning process of this thesis. Also, I would like to thank my loved ones, who have supported me throughout entire process, by keeping me harmonious, for endless patience, draft reading and helping me in the process of putting the pieces together. Garreth, Kaylee and Tamlyn you are the lights of my life and I will be grateful forever for your love.

ABSTRACT

We are living in what is being referred to as the information revolution, where the evolution of technology has and continues to have a pervasive impact on life and business. New technologies are being developed on a rapid scale that present several opportunities for businesses, however it also exposes them to several risks. As leadership and management of businesses have a professional, as well as a legal responsibility to govern businesses well, they must select and implement strategies and internal frameworks to limit the businesses exposure to risks, including Information Technology (IT) risks. In response to the rapid evolution of IT, specialist internal control frameworks have been developed and refined over time to address an entity's exposure to IT related risks at a strategic and operational level. Several of these frameworks, which are recognised and used globally, have been specifically designed in such a manner to ensure that leadership are able to dispel their corporate governance responsibilities whilst adding value.

As leadership of organisations have adapted the manner in which they address opportunities and risks, arising from evolving IT within an organisation, it is expected that the external auditor would also have adapted his/her audit approach to account for the impact of evolving IT on auditees. The external audit has, over time, evolved with significant social and economic advances and is today regulated and performed by making use of the International Standards on Auditing (ISA). The ISA have been updated to account for the pervasive impact that IT has on auditees. These updates have been included to account for the impact of IT throughout the audit process that the external auditor applies to conduct the external audit. These updates to the ISA address several considerations that the external auditor needs to make regarding the impact of IT on an auditee. However, when specifically considering the impact of IT when understanding the auditee and its environment, as well as the internal controls that are relevant to the audit, these updates to the ISA are broad in nature and do not necessarily provide the external auditor with the necessary detailed guidance. Several audit specialists have taken the general and application IT controls, included in the broad guidance of the ISA, and developed detailed control areas which the external auditor can use to address the impact of IT and the related internal controls on an auditee. Larger audit firms have developed internal frameworks that are used to address IT and its impact on the internal controls of auditees. However, in small and medium audit firms this is often not the case. Thus with the rapid evolution of IT and specialised internal control frameworks to govern IT, the question can be asked is, whether the ISA (together with the supporting guidance regarding IT), alone, suffice in enabling the external auditor of the small and medium audit firm to obtain a proper understanding of IT and address the impact of IT on their auditees.

The primary objective of this study was to develop a compressive approach that the external auditor of the small and medium firm, can apply to understand and address the evolving nature of IT and specialised IT internal control frameworks used by auditees when conducting the external audit. In order to achieve this objective the study first investigated what additional guidance is available to all external auditors when considering the impact that IT has on the auditee as well as which of the IT related internal controls that management have implemented are relevant to the audit. The additional guidance that was identified is in the form of more detailed control areas within the general and application IT controls that the external auditor must consider within each auditee. The study then considered whether these detailed control areas will address all of the control areas that management are considering by comparing it with the internal control areas of a specialised integrated IT internal control framework. Finally, by understanding the approach, required by the ISA, that the external auditor uses to assess internal controls which are relevant to the audit the author developed the comprehensive approach to address the impact of IT on an auditee in assessing control risk.

The findings showed that there is additional guidance, beyond the ISA, available to the external auditor when assessing the impact of IT on the internal controls of the auditee. This guidance is in the form of specific control areas within the general and application IT controls that the external auditor is required to consider when performing the external audit. However, when these control areas were compared with the control areas of a specialised integrated IT internal control framework, there were certain control areas, at a technology or operational level, which are not addressed through the control areas within the general and application IT controls. This confirmed the need for a comprehensive approach, to assist the external auditor of the small and medium audit firm, to assess the impact of IT on the auditee.

The ISA provides the external auditor with an approach to assess the impact of internal controls that are relevant to the audit on the risk of material misstatement by understanding the entity and its control environment, using the control objectives to identify key controls that are relevant to the audit and then testing the design and operation of those key controls. The author used a similar approach to develop a comprehensive approach to address the pervasive impact of IT, over and above the general and application IT controls already assessed, on the risk of material misstatement of the auditee taking into account the modern technology landscape. In the first step when understanding the entity and its control environment the author suggested that the IT governance impact on each of the areas included in the ISA when understanding the entity and its environment be used.

Secondly, the internal control objectives related to IT (as set out in the ISA) can be used to identify which of the controls identified through the understanding of IT governance are key controls and are relevant to the audit. Finally, the external auditor can then test the design and operation of those key IT controls that were identified as being relevant to the audit.

This revealed that there are likely to be IT related controls that are relevant to the audit at a strategic level (including general IT controls and strategic alignment through business imperatives), as well as an operational level (including application and technology IT controls). The comprehensive approach then requires the external auditor to test the design and operation of these relevant or key IT controls. It was found that the comprehensive approach can only be used by the external auditor of the small and medium firm, if applied at a strategic as well as an operational level. For this reason the external auditor of the small and medium firm, will need to have a more detailed understanding, or make use of an IT specialist, to assess the control risk impact at a technology level. To assist the external auditor of the small and medium firm, in gaining a more detailed understanding at a technology level the final finding of the study applied the comprehensive approach to common hardware and software components of IT systems found across several IT architectures.

By using the comprehensive approach developed the external auditor of the small and medium firm, will be able to address the control risks relating to the evolving nature of IT and the use of specialised IT internal control frameworks by management to govern IT when conducting the external audit.

UITREKSEL

Ons leef in ’n tyd wat beskryf word as die inligting revolusie, waar die evolusie van tegnologie ’n deurdringende invloed op die lewe en besigheid het en voort sal gaan om te hê. Nuwe tegnologieë word op 'n vinnige skaal ontwikkel wat 'n hele paar geleenthede skep vir besighede, maar hulle ook aan verskeie risiko's blootstel. Leierskap en bestuur van besighede het 'n professionele, sowel as wetlike, verantwoordelikheid om besighede goed te bestuur en daarom kies en implementeer hulle strategieë en interne beheerraamwerke om die besigheid se blootstelling aan risiko's, insluitende Inligtingstegnologie (IT) risiko's, te beperk. In reaksie op die vinnige evolusie van IT, is daar spesialis interne beheerraamwerke met die verloop van tyd ontwikkel en verfyn om die entiteit se blootstelling aan IT verwante risiko's op 'n strategiese en operasionele vlak aan te spreek. Verskeie van hierdie raamwerke word wêreldwyd erken en gebruik en is spesifiek op so 'n wyse ontwerp om te verseker dat die leierskap in staat is om hul korporatiewe bestuursverantwoordelikhede te bereik.

Aangesien die leierskap van organisasies, as gevolg van die evolusie van IT, die wyse waarop hulle IT geleenthede en risiko's aanspreek aangepas het, word daar ook verwag dat die eksterne ouditeur sy/haar ouditbenadering vir evoluerende IT sou aanpas. Die eksterne oudit het met verloop van tyd en met belangrike sosiale en ekonomiese vooruitgange ontwikkel, en word vandag gereguleer en uitgevoer deur gebruik te maak van die International Standards on Auditing (ISA). Die ISA is aangepas om die deurdringende impak wat IT op geouditeerdes het aan te spreek. Hierdie aanpassings sluit die impak van IT regdeur die ouditproses, wat die eksterne ouditeur gebruik om die eksterne oudit uit te voer, in. Die aanpassings aan die ISA sluit verskeie oorwegings wat die eksterne ouditeur in ag moet neem met betrekking tot die impak van IT op 'n geouditeerde. Die aanpassings aan die ISA is egter breed in aard en gee nie noodwendig die nodige gedetailleerde leiding nie, spesifiek met inagneming van die impak van IT wanneer die eksterne ouditeur begrip kry van die geouditeerde en sy omgewing, asook die interne beheermaatreëls wat relevant is tot die oudit. Verskeie ouditspesialiste het die algemene- en toepassings- IT interne beheermaatreëls, wat die breë riglyne van die ISA ingesluit is, geneem en spesifieke leiding geformuleer. Hierdie leiding sluit spesifieke beheergebiede in die algemene- en toepassings- IT interne beheermaatreëls, wat die eksterne ouditeur kan gebruik om die impak van IT en die verwante interne beheermaatreëls van 'n geouditeerde aan te spreek, in. Groter ouditfirmas het interne raamwerke, wat gebruik word om IT en die impak daarvan op die interne beheermaatreëls van hulle geouditeerdes aan te spreek, ontwikkel. In klein en medium ouditfirmas is dit nie noodwendig die geval nie. Dit kan dus bevraagteken word of die klein en medium ouditfirmas die nodige leiding het om IT en die impak daarvan op geouditeerdes volledig verstaan en aan spreek.

Die primêre doel van hierdie studie was om 'n omvattende benadering te ontwikkel wat die eksterne ouditeur van die klein en medium firma kan toepas om die evolerende aard van IT en die gespesialiseerde IT interne beheer raamwerke wat geouditeerdes gebruik te verstaan en aan te spreek. Om hierdie doelwit te bereik het die studie eers ondersoek ingestel oor watter bykomende leiding beskikbaar is vir alle eksterne ouditeure om die impak van IT op ’n geouditeerde sowel as watter IT interne beheermaatreëls, wat bestuur geïmplementeer het, relevant is tot die oudit. Die bykomende leiding wat geïdentifiseer was, is meer gedetailleerde beheergebiede binne die algemene- en toepassings- IT interne beheermaatreëls. Hierdie beheergebiede moet deur die eksterne ouditeur tydens elke oudit oorweeg word. Die studie het toe oorweeg of hierdie gedetailleerde beheergebiede al die beheergebiede wat bestuur sal oorweeg om IT te beheer insluit. Hierdie oorweging was gemaak deur die gedetailleerde beheergebiede te vergelyk met die interne beheergebiede van 'n gespesialiseerde IT raamwerk wat bestuur kan gebruik om IT volledig te beheer. Ten slotte, het die outeur die benadering wat die eksterne ouditeur gebruik om interne beheermaatreëls, wat relevant is tot die eksterne oudit, gebruik om ’n omvattende benadering te ontwikkel wat die impak van IT op die assessering van kontrole risiko van ’n geouditeerde aan te spreek.

Die bevindinge van hierdie studie toon dat daar wel leiding, bykomend tot die ISA, vir die eksterne ouditeur beskikbaar is wanneer die impak van IT op die interne beheermaatreëls van die geouditeerde beoordeel word. Hierdie leiding is in die vorm van spesifieke beheergebiede binne die algemene- en toepassings- IT interne beheermaatreëls wat die eksterne ouditeur moet oorweeg wanneer die eksterne oudit uitgevoer word. Met die vergelyking van hierdie beheergebiede binne die algemene- en toepassings- IT interne beheermaatreëls met die beheergebiede van 'n gespesialiseerde IT interne beheer raamwerk was daar sekere beheergebiede, op 'n tegnologie of operasionele vlak, wat nie aangespreek is nie. Daar is dus ’n behoefte aan 'n omvattende benadering wat die eksterne ouditeur van die klein en medium ouditfirma kan help om die impak van IT op die geouditeerde te evalueer.

Die ISA gee vir die eksterne ouditeur ’n benadering om die interne beheermaatreëls, wat van toepassing op die oudit is en wat ’n impak op die risiko van wesenlike wanvoorstelling het, te assesseer. Hierdie benadering is om die entiteit en sy beheer omgewing te verstaan, die kontrole doelwitte te gebruik om sleutel interne beheermaatreëls wat relevant tot die oudit is te identifiseer en daarna die ontwerp en implementering van sleutel interne beheermaatreëls te toets.

Die skrywer het 'n soortgelyke benadering gevolg om 'n omvattende benadering, wat die deurdringe impak van IT in 'n moderne tegnologie landskap, bo en behalwe die algemene- en toepassings- IT interne beheermaatreëls wat alreeds geassesseer is, op die risiko van wesenlike waanvoorstelling het te ontwikkel. In die eerste stap om die entiteit en sy beheer omgewing te verstaan het die skrywer voorgestel dat die IT beheer impak op elk van die areas wat die IAS uiteensit om die entiteit en sy beheeromgewing te verstaan, te oorweeg. Tweedens kan die IT verwante kontrole doelwitte (soos in die ISA uiteengesit) gebruik word om die sleutel IT interne beheermaatreëls wat relevant is tot die oudit te identifiseer. Ten slotte moet die eksterne ouditeur die ontwerp en implementering van sleutel IT interne beheermaatreëls toets.

Hierdie omvattende benadering het getoon dat daar IT verwante beheermaatreëls is wat op 'n strategiese en operasionele vlak op die oudit van toepassing is. Op 'n strategiese vlak sluit dit die algemene- IT interne beheermaatreëls en strategiese belyning met besigheid imperatiewe in. Op 'n operasionele vlak sluit die toepassings- IT interne beheermaatreëls en tegnologie interne beheermaatreëls in. Die omvattende benadering verlang daarna dat die eksterne ouditeur die ontwerp en implementering vir hierdie sleutel interne beheermaatreëls toets. Die omvattende benadering kan slegs deur die eksterne ouditeur van die klein en medium firma gebruik word as dit op 'n strategiese en operasionele vlak toegepas word. Die eksterne ouditeur sal dus IT in meer detail moet verstaan of 'n IT spesialis gebruik om die interne beheermaatreëls op 'n tegnologie vlak te assesseer. Om die eksterne ouditeur te help om 'n meer gedetailleerde begrip op 'n tegnologie vlak te kry het die finale bevinding van hierdie studie die omvattende benadering op algemene harde- en sagteware komponente van IT stelsels toegepas.

Deur gebruik te maak van die omvattende benadering wat ontwikkel is, sal die eksterne ouditeur van die klein en medium ouditfirma in staat gestel word om die beheer risiko's, wat verband hou met die evoluerende aard van IT en die gespesialiseerde interne beheerraamwerke wat bestuur van die geouditeerde gebruik om IT te bestuur, ten volle aan te spreek wanneer die eksterne oudit uitgevoer word.

TABLE OF CONTENTS

LIST OF FIGURES, TABLES AND APPENDICES

FIGURES

TABLES

APPENDICES

CHAPTER 1: INTRODUCTION AND BACKGROUND

1.1. Introduction and background

"Digital technologies — mobile, social, big data and cloud — are disrupting businesses everywhere by revolutionizing the role technology plays in our everyday lives." (Gartner, 2015) If businesses wish to remain relevant and profitable in the twenty-first century they will need to embrace the use of Information Technology (IT) in every area of the business extending from the vision and strategy through to operations and all the supporting structures. Although the context in which businesses are operating today is changing rapidly as a result of IT, there are certain principles which will remain constant across ever changing technological, social and economic landscapes. These principles specifically include the need for effective corporate governance of businesses where there is separation between leadership and management of businesses and the investors and other stakeholders. Leadership and management need to be held accountable for the manner in which they conduct business since leadership and management are often not the owners of the business. Stakeholders require confidence that their interests are being looked after. Corporate governance requirements and reporting structures facilitate this.

In South Africa the importance of good corporate governance is recognised by industry through the King commission which created the King Report on Corporate Governance, presently in its third release (IODSA, 2009). King III identified certain core principles that should be present in any corporate governance structure for an entity to function effectively. The implementation of these principles will vary in scale and complexity dependent upon the entities size and context. The importance of corporate governance was further validated in South Africa with the amendment to the South African Companies Act in 2008 (Republic of South Africa, 2008) to include certain principles from King III into the legislative requirements for companies dependent on their public interest. King III is principle based and the principles are intentionally broad in nature to allow leadership of the entity freedom in selecting and implementing frameworks and strategies to attain good corporate governance in the entity's context. Two key principles of King III are highlighted in this study. First the principle to govern IT appropriately and second the principle that the leadership of the entity demonstrates how it has designed and implemented a planned and systematic approach to manage risk which is supported by the entity's internal control, compliance and governance processes (IODSA, 2009).

King III acknowledges the importance of IT, focusing an entire chapter solely on IT governance and not merely considering it as part of the general principles regarding risk management and internal controls. King III requires the leadership of entities to take responsibility for strategic as well operational implementation of IT within the entity, more specifically in alignment with the entity's strategic objectives and strategies (IODSA, 2009). From this requirement it is evident that the use of IT within the entity is driven by the nature and objectives of the business and that leadership need to build processes and internal controls surrounding IT based on their business requirements. One of these business requirements is for the leadership to demonstrate that they have implemented sound risk management and internal controls. The leadership of organisations use internal control frameworks to assist them in demonstrating that they have met this principle of King III. The Committee of Sponsoring Organisations Framework (COSO) for internal control is a widely recognised and implemented internal control framework used to do so (Runino & Vitolla, 2014; COSO, 2013; Huang, Hung, Yen, Chang & Jiang, 2011). The reason for this is that the broad objectives of COSO align to the principles in King III in that they are the efficient and effective operations, compliance with laws and regulations and reliability of financial reporting. COSO, as an internal control framework, allows the leadership of the entity to govern the business effectively (business governance), as an element of corporate governance (COSO, 2013). The internal control framework implemented by an entity, such as COSO, includes all of the relevant internal controls, both manual and automated, which an entity will require to govern the entity appropriately. The specialised and complex nature of IT requires internal control frameworks, such as COSO, to be supplemented by IT focused internal control frameworks that address IT related risks and internal control specifically. Boshoff (2014) suggests that IT governance can only really be achieved effectively, as required by King III, if IT governance is considered at both a strategic and operational level similar to the manner in which business governance is only effective when implemented at both a strategic and operational level. If IT governance is required to be aligned to the entity's objectives and strategies then it follows that the strategic and operational aspects of business governance should be aligned to strategic and operational aspects of IT governance (Boshoff, 2014). Leadership of the entity will thus need to select and implement an internal control framework to achieve IT governance within the overarching internal control framework, such as COSO, that addresses both strategic and operational levels of IT governance. Whilst leadership of the entity selects and implements an internal control framework to dispel their responsibilities in terms of King III, King III acknowledges the need to provide stakeholders with assurance that the leadership and management of the entity has not only executed their corporate governance responsibilities appropriately within the entity's context, but has additionally reported the results appropriately in the financial statements.

This is demonstrated by the inclusion of the principle of combined assurance within King III. This principle highlights the need for assurance that is given to stakeholders which stems from management's objectives as well as internal and external assistance providers to the entity (IODSA, 2009). The external audit of the financial statements represents the external assurance providers of combined assurance referenced in King III which is the focus area of this study.

External audit, as an element of combined assurance, has given assurance to stakeholders, independent of management, regarding the performance of businesses and existence of assets for centuries (Flesher, Previts & Samson, 2005). The need for assurance from external auditors has intensified as the gap between leadership and management of entities and other stakeholders has grown with the introduction of capital markets in economies (Flesher *et al*., 2005; Imhoff, 2003). The importance of external audit has over time led to the profession as well as the processes followed by the profession in the execution of an external audit being formalised and prescriptive in nature (Byrnes, Gullvist, Brown-liburd, Teeter & Mcquilken, 2012; Robson, Humphrey, Khalifa & Jones, 2007). In South Africa external audit is governed by the International Standards on Auditing (ISA) and the external auditor navigates the audit process, as set out in the ISA, to effectively fulfil its purpose of enhancing the degree of confidence that users and stakeholders have in the financial statements (IAASB, 2014 ISA200:para. 3). A significant element of the audit process is planning the audit where the external auditor is required to consider the corporate governance of the entity, specifically including the internal control framework that leadership of the entity has implemented to govern the business. If it can be argued that each element of business governance, as an area of corporate governance, has a corresponding IT governance element then when the external auditor understands business (corporate) governance and the related internal controls he/she will further need to consider IT governance and the related internal controls. At present the ISA specifically require the external auditor to consider the impact that IT has on risks that are present within an auditee as well as the related internal control frameworks that leadership of the entity implemented to address those IT risks. These IT risks include the use of IT in financial reporting and other relevant areas of the auditee. The ISA specifically refer to general and application IT controls that have been implemented within the auditee's framework of internal control (IAASB, 2014 ISA315 (Revised): para. A103-105). The ISA give an overview of what general and application IT controls are; however the ISA do not outline specific control activities that the entity can implement, nor provides a framework against which it can be evaluated by the external auditor.

Similar to the manner in which internal control frameworks, such as COSO, are supported with IT specific internal control frameworks to support management in achieving IT governance, auditing experts have created common control areas that the external auditor needs to address in order to support the ISA overview of IT controls (Von Wielligh, Prinsloo, Penning, Butler, Nathan, Kunz, Matholo, O'Reily, Rudman & Scholtz, 2014; Marx, van der Watt & Bourne, 2014; Chang, Yen, Chang & Jan, 2014; Singleton, 2010; Sayana, 2002).

The nature and complexity of IT related controls which are being implemented by management to achieve IT governance, using internal control frameworks, have been streamlined, improved and become more complex with the evolution of IT and the nature of the underlying technology used by entities. One would expect that the overall approach that the external auditor applies when assessing IT controls as well as the control areas highlighted by the audit experts would also have evolved with the evolution of IT and the governance thereof. Larger audit firms have specialised IT divisions, which have IT specialists that are trained in IT control frameworks and provide the external auditor with support in assessing the IT controls of the auditee. However, small and medium audit firms may not have access to the breadth of in-house IT specialists in performance of their external audits. The Independent Regulatory Board for Auditors (IRBA) 2015/2016 Annual Report reported that there are 4,359 registered auditors in South Africa (IRBA, 2016). The majority of these registered auditors are small and medium sized practices as evidenced by the South African Institute of Chartered Accountants (SAICA) membership statistics for October 2016 which indicate that 85% of audit partners that are in public practice are at small and medium firms or are sole practitioners (SAICA, 2016). The part of the tertiary education curriculum dedicated to training future auditors that relates to IT controls is based on the ISA requirements and supporting guidance (University of Stellenbosch, 2016). As IT architecture becomes more complex, external auditors of the small and medium firm, without specialist IT auditors on their audit teams, may be at a disadvantage with knowledge limited to IT risks and controls that is based on the ISA and supporting frameworks. This, together with, the challenges that arise as IT architects, leadership of organisations and auditors do not fully understand the differences between the objectives, terminology and outputs that each uses (Julisch, Suter, Woitalla & Zimmermann, 2011), gives rise to the need for a comprehensive approach that the external auditor of the small and medium firm can apply to address the IT risks of an auditee.

1.2. Problem statement and research objective

The landscape and nature of IT has changed and continues to change which in turn exposes entities to new and sometimes unknown IT risks. Entities, of all sizes, have had to amend their approach to IT governance in order to respond to changing IT risks as well as realise the opportunities that IT creates. External auditors are required by the ISA to identify and respond to risks within the auditee, specifically significant risks of material misstatement, that relate to appropriateness of financial reporting when expressing an opinion on the historical financial information. These risks include those as a result of IT and its impact on the auditee. In the modern environment the question can be asked if external auditors, of small and medium firms, using the current requirements in the ISA and the supporting guidance, are equipped to appropriately identify and respond to the all of the significant risks that arise from IT and the governance thereof within an auditee.

The primary objective of this study is to provide the external auditor, of a small and medium firm, with a comprehensive approach to address control risks, which arise as a result of the impact that the evolving nature of IT has on auditees, when auditing historical financial information.

The primary objective can be expanded into the following secondary objectives:

1) Contextualise the impact that the evolution of IT has had on business and how entities use specialised frameworks to govern IT at a strategic and operational level.
2) Understand the external auditor's responsibilities in terms of the ISA regarding IT throughout the external audit of historical financial information.
3) Investigate what supporting guidance to the ISA is available to the external auditor when considering the impact that IT has on an auditee.
4) Assess if the external auditor of the small and medium firm, using the ISA and supporting guidance, appropriately addresses the impact of IT throughout the external audit of historical financial information by considering the ISA requirements in relation to how modern entities govern IT at a strategic and operational level.
5) Develop a comprehensive approach that the external auditor can use, in support of the current ISA requirements, to address all strategic and operational or technology level areas of IT and the governance there of at an auditee.

1.3. Scope limitations

External auditors operate in large, medium to small practices with differing levels of internal resource and expertise. Larger audit firms have in-house IT specialists and many of these larger firms have developed their own approaches to address IT risks of the auditee. However, this is not necessarily the case in the small and medium firms where the ISA requirements and supporting guidance are the sole basis used to consider IT risks of an auditee. This research only considers the ISA requirements, together with the supporting guidance, in the performance of the review of the available guidance to the external auditor and none of the firm specific approaches that, for example, the larger audit firms may have. Further, external auditors make use of Computer Assisted Audit Techniques (CAAT's) when conducting the audit. The use of these techniques in applying the comprehensive approach has been excluded for purposes of this study.

Entities use IT within their specific internal and external contexts and the rapid change and expanse of IT over time presents several possible IT architectures across entities (Mutsaers, van der Zee & Giertz, 1998). The hardware and software elements that are used across different IT architectures contain some similar elements however, remain unique dependent on the entity's requirements and context. For this reason in applying the comprehensive approach the research is limited to the hardware and software elements of the IT system that are commonly found across several IT architectures.

1.4. Organisational structure of the research

The research is presented in five chapters. Chapter 1 introduces the impact that IT has on business and the external audit of financial statements highlighting any potential gaps in what the ISA currently require the external auditor to consider and address in the performance of the external audit. Chapter 1 further presents the problem statement, research objective and sets out the limitations to the research as a result of the expansive and rapidly evolving nature of IT and the size of audit firms. Chapter 2 describes the research design and methodology including a detailed explanation of how the literature review was approached and executed in order to understand the historical research in the areas of business governance, IT governance and the impact thereof on external audit. Chapter 3 presents the literature review and highlights the relevance of the research objective and the impact of IT on the external audit. Chapter 4 presents the findings derived from the research methodology. Chapter 4 commences by discussing the additional guidance to the ISA that is currently available to assist the external auditor in assessing IT controls.

This is then followed by a consideration of whether the ISA, together with the supporting guidance, will suffice in providing the external auditor with an approach to comprehensively address IT risks of an auditee. Chapter 4 concludes by providing an overview of a proposed approach that the external auditor can apply when assessing IT of an auditee, followed by a detailed explanation of why it is considered appropriate and the approach itself. Chapter 5 concludes on the findings identified in Chapter 4 and highlights areas for further research.

CHAPTER 2: RESEARCH DESIGN AND METHODOLOGY

2.1. Purpose of the study

The aim of this study is to provide the external auditor of the small and medium sized firm, with a comprehensive approach to assist him/her in addressing the impact that IT, and the evolution thereof, has on the control risk of an auditee when auditing historical financial information. In order to achieve the aim of the study the research design included a systematic review followed by a process to develop the comprehensive framework which are explained.

2.2. Systematic review

The study commenced with a systematic review of the existing literature as Webster and Watson (2002) argue that an effective review of prior, relevant literature creates a firm foundation for advancing knowledge. They add, '*it facilitates theory development, closes areas where a plethora of research exists, and uncovers areas where research is needed*'. Okoli and Schabram (2010) confirms this notion by agreeing that a review of prior literature '*creates a solid starting point for all other members of the academic community interested in a particular topic*'. To achieve this solid starting point the author will apply Fink's definition (as cited Okoli & Schabram, 2010) of a rigorous stand-alone literature review that suggests following a systematic methodological approach, being explicit in explaining the procedures by which it was conducted, and being comprehensive in its scope by including all relevant items.

To focus the literature review, a concept-centred approach, as suggested by Webster and Watson (2002), was adopted using four of the five stages suggested by Sylvester, Tate & Johnstone (2013) as appropriate to the nature of the literature review performed. It should be noted that each of the four stages were carried out iteratively and incrementally. Initially, a broad selection of literature was made and the selection and number of articles and chapters included in this study were refined and reduced as the systematic review progressed.

1. *The Searching Stage:* In the searching stage a two pronged strategy was adopted. Firstly, the ISA themselves were reviewed to understand the legal and professional obligations of the external auditor in general and then more specifically to the impact of IT on the external audit. Secondly, the strategy for the searches of other pertinent areas to the study was extended by making use of the University of Arizona's search strategy builder tool to create broad search areas by assisting the author to clearly express concepts using several alternatives making the search more effective (University of Arizona, 2016). Search terms, included *inter alia*:

   - External audit
   - Risk identification and response
   - Key audit matters
   - Impact of IT on financial reporting
   - Business Governance & IT Governance
   - IT GAP
   - IT internal control framework
   - Internal control & COSO & COBIT
   - Control objectives – data integrity, validity, accuracy and completeness
   - Business processes
   - Access path & IT life cycle
   - IT architecture
   - Change in internal controls
   - General and application IT controls

   Library books, online bibliographic databases and professional subscriptions (such as Econolit, Science Direct, Ebsco host) were initially used to conduct the search. The search was then broadened to include informal web articles, whitepapers and other governance and audit related literature.

2. *The Mapping Stage (Or Paper Selection):* This entailed sorting and grouping identified literature into those dealing with similar concepts. For the purpose of this study, these concepts included, *inter alia*, Corporate and IT governance, IT revolution, external audit and risk assessment and IT governance and internal control frameworks. By grouping themes together the author was able to identify where the emphasis should be placed in the systematic review.

3. *The Appraisal Stage:* This stage entailed a detailed reading of each selected article, chapter, web reference, ISA, whitepaper or governance literature with the view of identifying the impact of the existing literature on the main concepts and aspects that could be considered and addressed with regard to corporate governance, IT governance, the evolution of IT, the role of the external auditor within corporate governance, the external audit and the evolution thereof over time.

4. *The Synthesis (Or Data Analysis) Stage:* The author combined, analysed, interpreted and concluded on key concepts that were identified in stage 3, The Appraisal Stage to support the research question.

The application of the concept centric four-stage process described above in conducting the systematic review, provided scientific rigour to the study. The systematic review highlighted the following core concepts that are used to present the findings in Chapter 3: Literature review:

- IT has evolved over time and this has changed the manner in which business is conducted.
- Leadership of organisations have a legal responsibly to apply strong corporate governance principles in managing the entity. Part of this responsibility includes responding to changes in the social, economic, legislative and IT environment that the entity finds itself in. This implies that if IT has changed the manner in which business is conducted it must also change the manner in which business is governed.
- Leadership of entities use internal control frameworks and processes to govern IT.
- External audit is a supporting pillar of the corporate governance structure and has advanced in the wake of ever changing economic, IT and social environments. This advancement has been facilitated by the formalisation of frameworks and legalisation that govern external audits.
- The ISA provide the process and requirements to conduct an external audit and follow a risk based approach which is largely driven by the auditee's internal and external context including how leadership governs the auditee.
- The question of if the ISA specific requirements for the external auditor fully address the evolution of IT and the changes in the way in which management is governing IT in a modern business.

2.3. Process followed in developing the comprehensive approach

Following the systematic review, steps one and two below enabled the author to identify whether the external auditor is currently addressing all of the risks that arise as a result of IT within an auditee when expressing his/her opinion on historical financial information. Once the author had identified that the external auditor is in fact not addressing all of the risks as a result of IT by using the current ISA requirements, and supporting guidance, the remaining steps (three and four) of the research methodology were followed to enable the author to propose a comprehensive approach that the external auditor can apply, in conjunction with the current ISA requirements, to address all of the risks that arise as a result of IT within an auditee.

Step 1: Investigate which supporting guidance is available to the external auditor when assessing the impact of IT on the external audit

The literature review (Chapter 3) found that the ISA do provide specific considerations that the external auditor has to apply when assessing the impact of IT on the external audit. Of these considerations the literature review (Chapter 3) highlighted that the area where external auditors require additional guidance is when assessing the entity's IT system and internal controls within the control environment. As a result it was necessary for the author to investigate what guidance is available to the external auditor. The investigation into how audit experts have analysed and explained how the external auditor should assess the entity's IT system and internal controls found that there is additional guidance in the form of detailed internal control areas that the external auditor needs to assess within the auditees IT control environment (Von Wielligh *et al*., 2014; Marx *et al*., 2014; Boynton & Raymond, 2006; Arens & Loebbecke, 1980). (The ISA together with the additional guidance will henceforth be referred to as the ISA.)

Step 2: Map the control areas included in the ISA regarding IT to the internal control areas identified by Goosen and Rudman (2013) that enable leadership to effectively and comprehensively govern IT

In order to assess if the ISA comprehensively address the impact of IT governance at a strategic as well as an operational level, the IT internal control areas in the ISA were mapped to the internal control areas identified by Goosen and Rudman (2013) which will enable leadership to govern IT. The control areas that were identified by Goosen and Rudman (2013) were selected for this analysis since the control areas are a combination of the control areas contained in three internationally recognised and used IT internal control Frameworks. These IT internal control frameworks are the Control Objectives for Information Technology (COBIT), International Organisation for Standardisation (ISO) 27001 and 27002 and Information Technology Infrastructure Library (ITIL). This mapping showed that there are certain internal control areas at an operational or technology level that are not addressed by the ISA.

Step 3: Using the approach that the external auditor uses to identify controls that are relevant to the audit, the author used a similar approach to understand which IT controls, over and above, the general and application IT controls according to the ISA's, are relevant to the audit

ISA 315 requires that the external auditor identify internal controls, manual and automated that are relevant to the audit (IAASB, 2014 ISA315 (Revised): para. 12 and 13). The literature review explained how the external auditor identifies and considers internal controls that are relevant to the audit by understanding the entity and its control environment, identifying key controls that achieve control objectives and will have an impact on the external auditors assessment of the risk of material misstatement by considering the design as well as the operating effectiveness of those controls. To develop a similar approach that the external auditor can use to identify which IT related internal controls are relevant to the audit, the author needed to identify a manner in which the elements of understanding the entity and its environment can be directly linked to the IT element that is included there in. A link needed to be made between the areas of business governance and the areas of IT governance. Before making this link, the author needed to identify the elements that are considered when understanding the entity and its control environment in order to identify internal controls that are relevant to the audit and can be mapped to the elements of business governance (Panel 1 in Table 1). A similar process had to be followed in understanding the IT governance environment (Panel 2 in Table 1). Boshoff (2014) provided a framework to align the areas of business governance and the areas of IT governance. By using each of the elements of IT governance (Panel 2 in Table 1) that are directly linked to the business governance counterpart (Panel 1 in Table 1) the external auditor will be able to identify the IT related internal controls that are relevant to the audit.

Step 4: Applying the comprehensive approach

The final step of this study discusses how the external auditor will apply the comprehensive audit approach, specifically the extended approach based on IT governance (Third section in Figure 1). In doing so the author applied the approach to hardware and software components that are commonly found across IT architectures.

CHAPTER 3: LITERATURE REVIEW

3.1. Introduction

The impact that the evolving nature of technologies has on businesses, how they are governed and its full impact on the external audit needs to be considered through various avenues that have been included in this systematic review. These areas include understanding how technologies have evolved over time; corporate governance and how businesses and their leadership have responded to evolving technologies; IT governance and IT governance frameworks; the role of external audit within corporate governance and finally the ISA requirements for the execution of the audit focussed on the impact of IT.

3.2. Evolution of IT

IT has evolved in a relatively short space of time and continues to transform and rapidly respond not only to the development of new technologies, but also to the changing needs of users, both private and professional (Mutsaers *et al.*, 1998). The advances in technologies and digitisation are considered to be profound and they are being referred to as the Forth industrial revolution (IODSA, 2016). For this reason, business and their leadership need to respond to opportunities and risks that IT exposes them to and in order to effectively govern IT, the historical and future evolution of IT needs to be considered.

Several authors have categorised the stages of the IT evolution using bases such as the architectures of business and IT as well as areas of computing (Boshoff, 2014; Aerts, Goossenaerts, Hammer & Wortmann, 2004; Cragg & Zinatelli, 1995). The common characteristics of each of the stages in the evolution of information technology across these authors include those set out below:

1. *Data processing* – where functionality of applications were initially driven by singular activities or tasks within organisations and were not integrated and batch processing updated separate data bases for each functional area within the organisation. The segregated nature of data processing caused a technological discontinuity when the technology evolved to the shared data base phase (Cragg & Zinatelli, 1995).

2. *Shared database* – where a clear separation between data bases and applications emerged. Functionality was business process driven rather than task driven; shared applications and shared data bases introduced the need for data base management systems. Data processing was no longer exclusively on mainframe computers and the personal computer made its first appearance. In its current form, companies are still using shared data bases for applications across functional areas within networks.
3. *Networks* – where organisations extended functionality across geographic locations connecting all functional areas of the business through the use of networks. Organisations also started communicating and linking with external organisations shifting towards the use of intranets and the internet. This shift resulted in the formation of the extended and virtual enterprise. Organisations were enabled to have web based functionality that was not restricted to the organisation or any specific physical location (Browne & Zhang, 1999).
4. *Mobile* – where the demand for instant, reliable, anywhere anytime functionality and information is and continues to be the driver for powerful technology on personal as well as professional mobile devices. Applications are developed based on specific user needs with the use of cloud storage which has and continues to improve operational effectiveness and efficiency (Gartner, 2015).
5. *Digital business* - Gartner, a leading research organisation, issues an annual cross-industry perspective on potentially transformative technologies that is summarised in the “Hype Cycle for emerging technologies”. The 2015 Hype Cycle for emerging technologies places a huge emphasis on moving forward to digital business and the convergence of people, business and things. The lines between physical and digital world are blurred as physical and digital assets share equal importance in the entity (Gartner, 2015; Luchetti, 2015).
6. *Autonomous* – According to Gartner the current horizon for IT Hype Cycle for emerging technologies ends with autonomous computing where IT is able to provide human-like or human- replacing capabilities to an entity (Gartner's 2015 Hype Cycle for Emerging Technologies Identifies the Computing Innovations That Organizations Should Monitor, 2015; Luchetti, 2015).

The rapid evolution in IT over time leads us to question what advancements lie beyond autonomous computing and what impact these advancements will have on life, business and the governance thereof.

3.3. Corporate Governance

For businesses to survive in the modern age, the leadership and management have to and need to continue to embrace the changes in technology together with the opportunities and risks that IT presents. As technology has progressed through the stages of the IT evolution so too has the manner in which entities do business, process, report and store information. The result is that the vast majority of entities are relying on IT systems, with varying degrees of dependence and complexity, to record, process, store and report financial and other pertinent company information. The leadership of organisations and legislators have acknowledged this by building IT into overall corporate governance structures. To understand the impact that IT has had on corporate governance structures, corporate governance itself first needs to be explored. Globally the methods by which entities are governed has become regulated and South Africa is no exception. In South Africa corporate governance is governed by South African company law and King III (IODSA, 2009; Republic of South Africa, 2008). The Companies Act of South Africa does not define or specifically refer to corporate governance, it does however, reference several of the principles included in King III and as such prescribes certain corporate governance principles, such as an external audit and social and ethics committee on companies, depending on their public interest (Republic of South Africa, 2008). King III on the other hand is not compulsory for all entities in South Africa; it is however, recommended for all entities in South Africa and has been included in the Johannesburg Stock Exchange Listing requirements (IODSA, 2009).

Corporate Governance is explained in King III to be about effective, responsible and ethical leadership that determines the organisation's strategic direction, assumes control of and takes overall responsibility for the entity (Von Wielligh *et al.*, 2014; Goosen & Rudman, 2013; IODSA, 2009). The IT Governance Institute (ITGI) supports this explanation by giving the origin of the term "Governance" as being derived from the Greek verb *kubernáo,* meaning "to steer" (ITGI, 2015). The ITGC further suggests that a governance system enables multiple stakeholders in an organisation to evaluate conditions and options, set strategic direction and monitor performance against the enterprise's objectives. Both King III as well as the ITGC place the responsibility of setting and maintaining an appropriate governance approach on the board of directors or equivalent body of an organisation. The individuals responsible for governance of the entity need to account for changes in the economy, business and society at large in planning the way forward to achieve success. As recent changes in business and the manner in which society functions are being driven by IT, IT governance has increased in prominence and importance within corporate governance structures.

3.4. IT Governance

The information revolution describes the impact that Information Technology has had and will have on the business cycle, economy and society at large (Rai & Lal, 2000). Information Technology within an organisation has evolved from supporting individual activities within a single organisation to now, not only being completely integrated across activities, but also across organisations. The introduction of the internet and the concept of mobility has directed organisations to converge internal IT hardware, software and networks with other IT devices and systems inside and outside of the organisation (Boshoff, 2014). King III acknowledges the pervasive impact that IT has had on every area of the organisation by devoting an entire chapter to IT governance (IODSA, 2009).

King III's definition of IT governance is that it can be considered as a framework that supports effective and efficient management of IT resources to facilitate the achievement of the company's strategic objectives (IODSA, 2009). IT Governance is thus not an isolated discipline but forms part of this larger corporate governance structure as it must link to the entity's strategic objectives (ITGI, 2015). For the leadership of any entity, represented by the Board of Directors, to fulfil its corporate and IT governance responsibilities, it selects and implements internal control frameworks and methodologies that relate to the organisation as a whole commencing with strategic IT governance and then filters down to include operational elements of the ever evolving IT system. To effectively govern IT the leadership of the entity needs to understand the changes to IT over time as well as anticipated future innovations.

King IV, released for public comment by the Institute of Directors in March 2016, echoes the emphasis that King III has placed on the importance and impact of IT and the continual evolution thereof on business in *Chapter 1: Introduction and fundamental concepts* and has dedicated *Principle 4.2* to *Technology and information governa*nce (IODSA, 2016). King IV, draft, maintains the focus areas of IT governance included in King III and further proposes expanding the responsibilities of the governing body of an entity regarding IT governance to include integrating people, technologies, information and processes in the digital business value chain and cyber-security risks to keep up with the evolution of IT (IODSA, 2016).

3.5. Use of internal control frameworks to achieve corporate and IT governance

King III bestows on the leadership of any organisation the responsibility to govern IT through the consideration of broad principles that the leadership need to apply. The principles in themselves will not enable the board of directors to govern IT and as such even require the board to delegate to management the responsibility for implementing an IT governance framework (IODSA, 2009). IT governance within an organisation forms part of a broader governance framework of internal control that enables the leadership of an entity to achive their governance objectives at a strategic and operational level. One must first understand the concept and objectives relating to internal control before applying similar principles to the governance of IT. The IAASB Glossary of terms defines internal control as:

> *The process designed, implemented and maintained by those charged with governance, management and other personnel to provide reasonable assurance about the achievement of an entity's objectives with regard to reliability of financial reporting, effectiveness and efficiency of operations, and compliance with applicable laws and regulations. The term "controls" refers to any aspects of one or more of the components of internal control.* (IAASB, 2014 Glossary of terms)

The above definition of internal control is broad and includes all elements of the internal control system whether manual or IT related. The definition places the responsibility of designing, implementing and maintaining the system of internal control with management. This notion is supported by the responsibility placed on the leadership of the organisation for good corporate governance, specific ally including the system of internal control, by King III (IODSA, 2009).

3.6. COSO Internal Control – Integrated framework

The internal control frameworks that are implemented by the leadership of the organisation will need to achieve the broad control objectives set out in the IAASB Glossary of terms. These control objectives are to provide reasonable assurance about the achievement of an entity's objectives with regard to reliability of financial reporting, effectiveness and efficiency of operations, and compliance with applicable laws and regulations. These broad control objectives are similar to those set out in the COSO (2013) which is a widely used and recognised framework for internal control (Runibo & Vitolla, 2014; Huang *et al.*, 2011).

COSO not only provides control objectives but is a commonly accepted tool that is used by entities to achieve the control objectives as a whole (IAASB, 2014 ISA315; Gheorghe, 2010; Klann & Watson, 2009; Yang, 2004). The components of COSO's internal control framework are inter-related and need to be addressed in their entirety to achieve the objectives of internal control. The first component, *control environment*, provides the foundation for all of the other internal control components and sets the tone at the top of the organisation. It includes the integrity, ethical values, competence, philosophy, and operating style of the firm's managers and employees. The second component, *risk assessment*, is the identification, examination, assessment and management of (operating, economic, industry, regulatory) risks that may prevent an organisation from achieving its objectives. Management implements *control activities* within the information systems and processes (the third component) to mitigate the identified risks. Control activities include segregation of duties, performance reviews, information processing, physical controls and approvals. The fourth component*, information and communication*, refers to the relevant, timely and quality generation and communication of information both internally and externally. The final component, *monitoring*, is the continual evaluation of the other components' effectiveness (IAASB, 2014 ISA315; COSO, 2013; Gheorghe, 2010; Klann & Watson, 2009).

COSO follows a principle based approach that provides flexibility in application and requires that management use their own judgement with specific reference to the business context to design the most appropriate system of internal control, both manual and IT related, that addresses all the elements and internal control objectives included in COSO (2013). COSO in itself however, does not address IT governance internal controls in sufficient detail to enable management to use it as a standalone framework for achieving IT governance in support business governance (Chang *et al.*, 2014). It is common business practice to supplement the COSO framework with other recognised internal control frameworks to achieve all of management's corporate and IT governance principles (Rubino & Vitolla, 2014).

3.7. IT Governance Frameworks

The Information Systems Audit and Control Association's (ISACA) global look at best IT audit practices highlighted IT governance frameworks that organisations are currently using. The majority of organisations surveyed use of the COBIT as the basis for their IT audit risk assessments. COSO, ISO and ITIL are also used by organisations to a lesser degree in governing IT and assessing IT related risks. (ISACA & Protiviti, 2015) Each of the highlighted frameworks have differing areas of focus when governing IT.

COBIT addresses the IT system in its entirety from strategic alignment, daily operations, and IT system development to service delivery and support through the use of processes and structure from the organisations point of view. (ISACA, 2014) COSO, as discussed above, provides an overarching framework for internal control including control objectives that are supported by additional IT governance frameworks (3.6) ITIL provides best practices in the service delivery by the IT department, from the IT department's point of view, to clients as well as the organisation itself as their key client. ITIL addresses areas including service strategy, design, transition, operations and continual improvement. (Sanker, 2013; Goosen & Rudman, 2013) ISO, specifically ISO27001 and ISO27002, address risk management policies and preventative, detective and corrective internal controls to ensure security over the entire management information system. Including policies, human resources, physical security, access control, data transfer, use of third parties, system acquisition, development and maintenance, incident management, business continuity and compliance (Goosen & Rudman, 2013).

Each of these IT governance frameworks can assist the leadership of the organisation to achieve IT governance; however, when applied individually Goosen and Rudman (2013) highlighted there may be risk that the IT systems and related internal controls that are implemented at a strategic and operational level are not in line with the entity's unique strategic objectives and strategies. Goosen and Rudman (2013) suggested that the control areas highlighted in COBIT could be enhanced by integrating them with the control areas in ITIL and ISO 27001 and ISO 27002 to assist management in achieving alignment between the IT systems and related internal controls and the entity's unique strategic objectives and strategies at a strategic as well as an operational level. By eliminating areas of overlap between the four frameworks, they developed a comprehensive list of control areas (separated between those at a strategic and those at an operational level) and referred to as the "Integrated Framework" (Goosen & Rudman, 2013).

The control areas highlighted in the “Integrated Framework” at a strategic level focus around aligning IT resources, systems and operations with the business strategies; setting appropriate policies and procedures within all areas of the IT function; controlling access to IT assets; risk assessment of IT related risks; project management of IT projects; incident and continuity management within IT and finally compliance, financial and human resource management regarding IT. The detailed control areas are discussed below (Goosen & Rudman, 2013).

- **Determine business policies and strategies:** The documentation and communication of management’s vision mission and strategic direction for the organisation.
- **Implement business-IT alignment procedures:** The alignment of IT objectives to organisations objectives enabling IT to add value to the organisation.
- **Service level management procedures:** The management of IT resources in line with the organisations strategic objectives while continually monitoring and improving service delivery to ensure customer satisfaction.
- **Implement accurate IT resource management:** The design and implementation of the current and future IT architecture and use of IT resources in line with the organisations strategic objectives, risk analysis and economic feasibility.
- **Procurement management:** The setting and implementation of a formal procurement policy to ensure the quality and appropriateness of IT supplier services.
- **Access controls/ Security management:** The design and implementation of physical and logical access controls to protect IT assets against physical and environmental dangers as well as unauthorised access to the IT system as a whole or individual applications therein. Including network security controls, such as firewalls, controlling mobile code, and controlling the network connections.
- **The acquisition and development of an information system and maintenance controls**: The setting and implementation of an acquisition and development policy specifically including access controls and quality control throughout the phases of development and approval.
- **Project management:** Project management of entire IT projects from agreeing deliverables, allocating resources, assessing quality control and testing, implementation and post implementation review.
- **Implement an information management system:** The design and implementation of internal controls through the use of an information management system to ensure that financial and operational data is integrit and remains accurate, available, and confidentiality is ensured.

- **Financial management:** The valuing, monitoring and controlling of the investment in IT assets, including measuring the return on investment as well as the correct cost allocation based on use of the IT assets.
- **Risk management process:** The assessment of risks relating to IT service design, delivery and processes with the development of an IT security plan to address risks identified.
- **Change, release and deployment management:** The setting and implementation of a set standard for all changes to the IT system, procedures, policies, processes, and configuration settings.
- **Human Resource Security:** The appointment of appropriately qualified staff to the matching position within the IT department. Monitoring of performance of IT personnel and continual relevant IT training to all personnel using the IT system.
- **Problem Management**: The implementation of a central service desk for all problems encountered as well as security incidents related to the IT system.
- **Business Continuity Management:** The design of an IT disaster recovery plan specifically including the establishment of off-site back-up facilities.
- **Compliance Requirements:** Consideration and implementation of controls to adhere to relevant laws and regulations. These controls should also take technical compliance standards and audit requirements into consideration.
- **Configuration Management**: The design and implementation of IT controls surrounding the configuration of IT assets. These controls should ensure that the IT configuration settings are correct in terms of the organisations policy and that any invalid configurations are corrected.

Should all of the strategic level control areas highlighted by Goosen and Rudman (2013) be addressed, the leadership of the organisation will have achieved IT governance at a strategic level. However, this will not address the governance of IT at an operational or technology level in the actual hardware and software components that are included within the IT system. To do so, Goosen and Rudman (2013) recommend identifying access paths and individual components therein and then implementing configuration controls for each of the components identified, these are explained below.

- **Identify access paths:** An access path can be used by management as a tool to govern IT at a technology level (Goosen & Rudman, 2013). Each time access is granted to the IT system either for the purpose of processing transactions included in a workflow, extraction of information or IT support or maintenance, the concept of an access path needs to be considered (Killmeyer, 2006). Boshoff (1990) defines an access path as: *A user performs computerised activities by activating an access path. An access path is formed by the various IT components that need to be activated in order for a typical user (business, IT or otherwise) request (functionality, data or otherwise) to be executed, in order to access computer controlled resources.* The ISACA glossary of terms supports Boshoff's definition as it explains an access path to be the logical route that an end user takes to access computerised information and it typically includes a route through the operating system, telecommunications software, selected application software and the access control system (ISACA, 2014). Once each of the access paths and the individual hardware and software components therein have been identified, configuration controls need to be implemented for each of the identified components.
- **Implement configuration controls:** These configuration controls (which can alternatively be referred to as IT Life cycle tasks) include those controls that need to be implemented at each stage of an access path component's life cycle (Goosen & Rudman, 2013). This principle has been supported by Julisch *et al.* (2011) when referring to the life cycles of applications and their internal controls. Boshoff (2014) expands the IT life cycle tasks to include the functions to configure, build, operate and maintain each component of the access path (Goosen & Rudman, 2013). These IT life cycle tasks are:
  - *Computer hardware is built* by assembling the various components to enable it to accept an operating system in order to function as a computer.
  - *Computer software build* refers either to the process of creating and converting source code files into standalone software artefact(s) that can be run on a computer, or the result of doing so. One of the most important steps of a software build is the compilation process where source code files are converted into executable code.
  - *Setup or installation of a program* (including drivers, plugins, etc.) is the act of putting the program onto a computer system so that it can be executed, including the initial software parameters that are to be set for the installation.

- *Configuration of computer software* creates configuration files, or configs that configure the initial settings for some computer programs. They are used for user applications, server processes and operating system settings. These configuration settings can also be changed at a later date.
- *Operating a computer* entails overseeing the smooth running of a computer/device and intervening by stopping, restarting services and/or the whole computer.
- *Computer maintenance* ensures that computers/devices are repaired or the software upgraded to ensure optimum performance and reliability.

Using the components of the access path and the supporting configuration controls will enable management to implement IT governance at an operational or technology level, which as required of King III (Goosen & Rudman, 2013) and address each systems risk. Once the leadership and the management of an organisation have implemented the necessary internal control and IT governance frameworks within an entity they will be able to demonstrate that they have dispelled their responsibilities in terms of King III. This alone will however, not be robust enough to assure stakeholders that management is in fact doing so. This is where the principle of "combined assurance" steps in to assure stakeholders of the organisation that effective corporate and IT governance is in fact taking place.

3.8. Role of external audit within corporate governance

Corporate governance, including IT governance, is supported by combined assurance provided to stakeholders that the leadership and management of the entity are in fact governing and reporting this financial performance and position appropriately. *Principle 3.5* of King III introduces the concept of a combined assurance model as a recommendation for good corporate governance practice. The combined assurance model aims to optimise the coverage obtained from management and internal and external assurance providers to address risks affecting the company. According to the PriceWaterhouseCoopers report on implementing combined assurance, in the era of King III, combined assurance is achieved through three lines of defence, firstly being management oversight; secondly being a formal and effective risk management framework and thirdly independent and objective assurance (PWC, 2010). Independent and objective combined assurance to the stakeholders of the entity regarding the financial statements, internal control and other governance areas of the entity will enable, amongst others, effective board or management decision making and support investor confidence. Included within independent and objective assurance are all of the internal and external assurance providers to a particular entity; which includes external audit.

King III and King IV, draft, echo the sentiment that external audit plays a key role in achieving combined assurance within good corporate governance (IODSA, 2016; IODSA, 2009).

In a South African context despite the fact that compliance with King III is voluntary, unless listed on the JSE, South African company law prescribes external audits of historical financial information for companies that are of public interest (Republic of South Africa, 2008). Legal entities can include a mandatory audit requirement within their founding documents or contractual obligations, for example with funders, who require an external audit on the financial statements. Understanding the origin, purpose, objective and role of external audit and the impact of corporate and IT governance thereon are thus of significance for a broad number of entities in South Africa.

3.9. Origin and evolution of external audit

The notion of an external audit to provide assurance arose alongside the emergence of agency of asset challenges - when those owning assets and those managing assets were not the same individual. This concept has thus been in existence for several centuries where the owners of assets required some form of evidence that assets were not being misappropriated (Flesher *et al*., 2005). As the economic structure of civilisation evolved from self-funding to the introduction of the concept of financing in business, so too did the need for accurate financial reporting and the external audit thereof. However, the formalisation of external audit procedures to verify financial information and existence of assets were initially largely driven by industrialisation and spearheaded by the railways. This was where, for the first time, investors and corporations began to participate in the stock market and the separation between ownership and management deepened. The railways drove the process of fraud prevention, financial accountability, cost accounting and operating effectiveness forward (Byrnes *et al*., 2012; Matthews, 2006; Flesher *et al*., 2005; Bryer, 1993). From these corporate and audit beginnings, the pool of thought that corporate governance and the need for an external audit as part of a corporate governance structure are essential to the effective functioning of capital markets arose and continue to exist today (Imhoff, 2003; Cohen, Krishnamoorthy & Wright, 2002). Formalised methodologies, structures, standards and legislative requirements define and drive the role, responsibilities, process and outputs of the modern day external auditor (Byrnes *et al*., 2012; Robson *et al*., 2007). Changes, improvements and the modernisation of corporate governance as well as external audit have been, and continue to be driven by changes to business and society over time; however, the core objective behind external audit have not.

The methodologies and frameworks used to perform the external audit have been questioned and improved upon to reflect the changing social, economic and business landscape globally (Robson *et al*., 2007). Academic research as well as practical execution within the external audit environment continually and proactively facilitate this questioning process through assessing the relevance, scope, efficiency and effectiveness of the external audit and proposing enhancements moving forward. Significant enhancements to and research in the way an external audit is executed to date include the shift from merely certifying balances to following a risk based audit methodology in the early 1990's.

The use of the computer in the performance of the audit and the impact of the use of the computer by auditees and the increased focus on fraud and internal control with the passage of the Sarbanes-Oxley Act of 2002 in United States of America (Byrnes *et al*., 2012; Fraser & Pong, 2009; Janvrin, Bierstaker & Lowe, 2008; Robson *et al*., 2007). More recently, specific elements of the audit approach applied by the external auditor have been examined which include the effective and appropriate use of statistical sampling in the performance and assessment of audit procedures performed (Swanepoel, 2013), areas of corporate governance considered by the external auditor (Cohen *et al*., 2002), improvements to the audit approach in specific industries and the use of experts in the performance of the external audit (Von Wielligh, 2006).

Of all of the enhancements that have been made to the external audit, the focus area of this study is the impact that IT has and continues to have on the external audit. The introduction of computers and IT systems drastically amended the way in which organisations account for transactions moving from a manual documentation and recording process to a semi or even fully automated one. Audit evidence is no longer merely in tangible assets, documents and records but now additionally in electronic data and reports. Initially external auditors audited around the computer assessing transactions and information being inputted onto the computer and then outputs from the computer rather than looking into the actual computer itself. This processes initially sufficed, however as IT systems and the supporting technology have evolved and continue to evolve, the risks that present themselves have increased in significance and complexity and in the early 1960's Kaufman presented the idea that the external auditor needs to start auditing through the computer as opposed to around the computer (Kaufman, 1961). The impact that the internal controls within and surrounding the computer have a significant impact on the quality and reliability of the audit evidence that is presented to external auditors and thus need to be included within the external auditors audit approach.

The nature and complexity of IT systems as well as the internal controls that need to surround them have advanced as IT has evolved and is thus expected to have an ever increasing impact on the external auditors approach. To consider the impact that IT has had on the external audit, the purpose and process which external auditors use when performing an external audit first needs to be understood, including specific requirements included in the ISA regarding IT.

3.10. Purpose of an external audit

External audit forms an essential element of any governance structure as it supports users of the financial statements to have confidence in management's corporate governance, including IT governance, of the entity (Imhoff, 2003; Cohen *et al.*, 2002). If external audit is to fulfil its role within the governance structure, in the modern and South African context, it is necessary to have a clear understanding of what the purpose of an external audit is. The specific purpose of an external audit as defined in ISA 200: *Overall objectives of the independent auditor and the conduct of an audit in accordance with international standards on auditing (IAASB, 2014* ISA200:para. 3), is to enhance the degree of confidence to the intended users of the financial statements. This is in direct correlation to the requirement to give assurance to the stakeholders in King III. This confidence is supported by the reasonable assurance that the external auditor expresses that the financial statements, prepared by the management of the organisation, as a whole, are free of material misstatement in terms of the applicable reporting framework (IAASB, 2014 ISA200:para. 11(a)). The financial statements that are prepared by management of the entity, who assert that they represent the results of operations, cash flows for a specified period of time and the financial position of the entity at a specific date. To do so the external auditor will need to apply the audit process and principles as set out in the ISA.

3.11. The audit process

The audit process is a series of activities and procedures that are set out by the ISA and that the external auditor follows to enable him/her to express an opinion on the annual financial statements, prepared by management of the entity (Von Wielligh *et al.*, 2014). This opinion is based on the evidence that the external auditor gathers to support the assertions that management has made regarding the financial statements. Throughout the audit process the external auditor applies a risk based approach in the performance of his/her duties, a theme which is evident as explained in each of the stages in the audit process (Byrnes *et al.*, 2012; Fraser & Pong, 2009; Janvrin *et al.*, 2008; Robson *et al.*, 2007).

The stages of the audit process include pre-engagement activities, planning activities, execution or performing the planned audit procedures and evaluating the audit evidence or concluding (Von Wielligh *et al.*, 2014; Marx *et al.*, 2014). These stages are explained as:

3.11.1. *Pre-engagement activities*

The external auditor determines if he/she wishes to accept the audit engagement; as part of this decision making process the external auditor will consider the potential risk of misstatements.

3.11.2. *Planning activities*

The planning activities on an audit include obtaining an understanding of the entity and its environment, including internal control; assessing audit risk and developing an audit approach that will enable the external auditor to gather sufficient evidence that the financial statements are not materially misstated.

3.11.2.1. Understanding the entity and its environment

The planning phase of the audit commences with understanding the entity and its environment, including the entity's internal control, with the purpose of identifying and assessing the risk of material misstatement (IAASB, 2014 ISA200:para. 7). *ISA 315 (Revised) Identifying and assessing the risks of material misstatement through understanding the entity and its environment* requires that, when understanding the entity and its environment, the external auditor places the auditee into context by understanding elements in and surrounding the auditee including the industry and regulatory environment, the nature of the entity specifically including governance structures, financing structure, objectives and strategies and the selected accounting framework of the auditee (IAASB, 2014 ISA315 (Revised): para. 11).

3.11.2.2. Understanding the entity's internal control

Over and above each of the elements within the entity and its environment, the external auditor needs to obtain an understanding of the entity's internal control, which directly aligns to internal control required by King III (3.5) and the elements of internal control included in ISA 315 are identical to those included in COSO (3.6). Once the system of internal control has been understood the external auditor needs to identify those internal controls that are relevant to the audit. The controls that are relevant to the audit are those controls that support management in asserting that the financial statements are appropriate (IAASB, 2014 ISA315 (Revised): para. 12 and 13).

Not all internal controls will support management in doing so as they relate to the other broad objectives of internal control being efficient and effective operations and compliance with laws and regulations. The ISA presents management of the entity with specific qualities that need to be present within the financial statements and financial reporting of the entity that demonstrate that the financial statements are appropriate. These qualities are referred to as management assertions (IAASB, 2014 ISA315 (Revised): para. A124). The ISA separate these management assertions into those assertions made over transactions included within and balances on the financial statements presented for external audit. These management assertions include occurrence, completeness, accuracy, cut-off, classification and presentation of transactions as well as existence, rights and obligations, completeness, accuracy, classification and presentation of balances in the financial statements (IAASB, 2014 ISA315 (Revised): para. A124). When understanding the entity's system of internal control only specific management assertions are relevant as not all of the management assertions regarding the financial statements can be achieved by the system of internal control of an entity. The relevant management assertions are those that can be linked to the specific control objectives that management uses when designing and implementing a system of internal control, being completeness, accuracy and validity of all transactions or events that have taken place in the financial period covered by the financial statements (Von Wielligh *et al*., 2014; Boshoff, 2014; Boynton & Raymond, 2006; Arens & Loebbecke, 1980). The external auditor considers which controls are relevant to the audit by considering which controls best achieve the control objectives. Using the controls that are relevant to the audit, the external auditor assesses if the controls are designed effectively to achieve the control objectives and then uses this in assessing control risk within the risk of material misstatement.

3.11.2.3. Assessing audit risk and developing an audit approach

Using this understanding of the entity and internal controls that are relevant to the audit the external auditor is able to identify and assess the risks of material misstatement and formulate an audit approach moving forward to address the risks identified.

3.11.3. *Execution (Performing the planned audit procedures)*

The external auditor uses the audit approach developed through the planning phase of the audit process and obtains audit evidence to support the audit opinion. Audit evidence obtained needs to be sufficient to address each of the management assertions for transactions and balances included in the financial statements (3.11.2.2). Audit evidence obtained is in the form of the results of audit procedures performed at the auditee which include test of controls and substantive procedures.

Test of controls are audit procedures that test the operating effectiveness of the internal controls that have been identified by the external auditor as being relevant to the audit by achieving a control objective and assessed as being designed effectively as part of the control risk assessment performed in the planning phase of the audit process (3.11.2.2). Substantive procedures, which can either be tests of detail or analytical review procedures, focus on amounts in and disclosures on the financial statements (IAASB, 2014 ISA330:para. 8 & 18; IAASB, 2014 ISA500:para.A10).

3.11.4. *Reporting (Evaluating the audit evidence)*

The external auditor assesses if the results of audit procedures performed will indeed reduce audit risk to an acceptable level to support the audit opinion that is expressed. If not, further procedures will be performed before the audit opinion will be expressed.

Throughout the audit process the external auditor follows a risk based approach and audit risk is the basis for the understanding of the entity, drives the audit approach and finally the assessment of the results of the audit procedures before expressing the audit opinion. Thus before one can consider the current ISA requirements regarding the impact of IT on the audit process, the external auditor must understand audit risk.

3.12. Audit risk

The external auditor plans and performs the external audit using a risk based approach to reduce audit risk to an acceptably low level. Audit risk is defined in ISA 200 to be the risk that the auditor expresses an inappropriate unqualified opinion on the financial statements when the financial statements are in fact materially misstated (IAASB, 2014 ISA200:para. 13(c)). To ensure that audit risk is managed and maintained at an acceptably low level, the entire audit approach throughout the audit process and the execution thereof is driven by audit risk. ISA 200 expands audit risk to be a function of the risk of material misstatement and detection risk. The risk of material misstatement, is the risk that the financial statements are materially misstated prior to audit. This risk is beyond the control of the external auditor and comprises of inherent risk and control risk. Inherent risk is the risk that a class of transaction, account balance or disclosure is materially misstated before any consideration of internal controls. Control risk is the risk that a misstatement in a class of transaction, account balance or disclosure is not prevented, detected and corrected in a timeous manner by an entity's system of internal control (manual and automated) (IAASB, 2014 Glossary of Terms).

The risk of material misstatement is assessed by the external auditor ranging between high, medium or low as part of the planning phase of the audit process (Huang *et al.*, 2011).

The second element of audit risk, detection risk, is the risk that the external auditor's procedures do not reduce audit risk to an acceptably low level (IAASB, 2014 ISA200:para. 13(c), (e), (n)(i) and (n)(ii)). Within the planning phase of the audit, detection risk represents the auditor's planned response to the assessed level of material misstatement to keep the level of audit risk that the auditor is willing to accept at an acceptably low level (Huang *et al.*, 2011).

When combined with the risk of material misstatement these elements of audit risk will drive the audit approach and the type of audit procedures performed in the execution phase of the audit process.

In the reporting phase of the audit process the external auditor assesses if the results of the audit procedures performed support the initial assessment of control risk and the level of detection risk that he/she is willing to accept. If it does, the external auditor issues his/her audit opinion. If not, the external auditor will then amend the audit control risk assessment and the level of detection risk he/she is willing to accept and extend the audit procedures accordingly. Once the results of the extended audit procedures are finalised the external auditor then expresses his/her opinion.

3.13. Impact of IT within each phase of the audit process

The ISA have acknowledged the fact that IT has and continues to have a pervasive impact on the audit by considering IT in each of the phases of the audit process through considerations to be made by the external auditor as well as prescribed actions regarding IT that the external auditor needs to take. An overview of the ISA requirements for each phase of the audit process is discussed in the following subsections.

3.13.1. *Pre-engagement activities*

An external auditor has a professional and ethical responsibility to only accept engagements, audit or otherwise, that he is competent to perform. This will ensure that his/her clients receive a proficient, professional service and will uphold the dignity of the profession (SAICA, 2015; IAASB, 2014 ISA210).

In this context the external auditor needs to be aware of the IT system that has been implemented at the auditee and the external auditor must either have the necessary degree of proficiency in IT in-house or will need to appoint an IT specialist or expert prior to accepting the engagement (Vasarhelyi & Romero, 2014). There is a growing awareness that the external auditor needs to attain a certain level of competency in the IT area to enable him/her to perform external audits; however, the level of this competency is however not clearly defined (Byrnes *et al.*, 2012; Janvrin *et al.*, 2008). Given the pervasive nature of IT and its impact on business, auditors can no longer assume that auditing around the computer, without considering the technology and internal controls therein, will suffice in addressing the risks that arise from IT within an auditee. This implies that in applying the competency requirement, regarding assessing the risk of misstatement as a result of IT within the auditee, the external auditors in the small and medium firm may require more detailed guidance than the ISA in the form of a comprehensive approach to assist them.

3.13.2. *Planning activities*

The planning activities on an audit include obtaining an understanding of the entity and its environment, including internal control; assessing audit risk and developing an audit strategy and approach. The impact that IT has on each of these activities varies in significance based on the nature of the activity.

3.13.2.1. Understanding the entity and its environment

When understanding the entity and its environment ISA 315 gives an overview of areas to that the external auditor needs consider when performing risk assessment procedures, the ISA does not however, provide detailed guidance. The impact that IT has had on the broad areas of understanding the entity is as follows:

- **Nature of the industry and the entity's objectives and strategies:** IT has impacted each industry uniquely and the external auditor will need to assess what that impact will be on the auditees industry. The entity's objectives and strategies will need to consider the risks and the opportunities that IT present within the entity's industry.
- **Financing structure and accounting framework:** IT will have little or no impact on the financing structure or the accounting framework that is adopted by the entity. It will however have an impact on the transactional or accounting process used to report information that is included in the accounting framework as well as how data is stored and maintained, discussed in understanding the entity's internal controls (3.1.13.2).

- **Regulatory environment and governance structures:** The recent changes in the global legislative landscape and more specifically in South Africa regarding privacy of personal information through the implementation of The Protection of Personal Information Act 4 of 2013 (Republic of South Africa, 2013) and the changes in King III and King IV regarding IT will impact the entity's governance structures and internal processes to ensure compliance. This filters down to the entity's internal control and how the entity governs IT as required by King III.

3.13.2.2. Understanding the entity's internal control

Over and above each of the areas described in the previous section the external auditor is required to obtain an understanding of the entity's internal control which will translate into the external auditor's assessment of control risk (3.12). The external auditor's assessment of control risk hinges on management's internal processes and internal control frameworks selected and implemented by management, including both manual and automated controls, for management to achieve corporate as well as IT governance (3.5). ISA 315 makes reference to the fact that the use of IT, as it forms part of the internal processes and internal controls that management have implemented within the elements of the COSO is relevant to the external auditor's understanding of the entity including internal controls. Further, ISA 315 gives more detail regarding the impact that IT has had on the way the entities do business, the way that financial information is captured, recorded, stored and reported upon and the internal controls that the leadership of the entity implement regarding IT. The specific considerations and guidelines regarding the impact that IT has on internal control are:

1. The external auditor needs to obtain an understanding of internal control relevant to the audit which include both the manual and automated procedures that are used to initiate, record, process and report transactions that are relevant to performance of the audit (IAASB, 2014 ISA315 (Revised): para. 12; 18 & A60-A61; Center for Audit Quality, 2014).

2. The use of IT can generally benefit internal controls by enabling the entity to:
    - Consistently apply predefined business rules and perform complex calculations in processing large volumes of transactions or data;
    - Enhance the timeliness, availability, and accuracy of information;
    - Facilitate the additional analysis of information;
    - Enhance the ability to monitor the performance of the entity's activities and its policies and procedures;
    - Reduce the risk that controls will be circumvented; and

- Enhance the ability to achieve effective segregation of duties by implementing security controls in applications, databases, and operating systems.

(IAASB, 2014 ISA315 (Revised): para. A62)

3. The use of IT can expose the organisation to additional risks that need to be considered and addressed in the governance of IT as well as by the external auditor. These factors are expanded upon in ISA 315 to include:
   - Reliance on systems or programs that are inaccurately processing data, processing inaccurate data, or both;
   - Unauthorized access to data that may result in destruction of data or improper changes to data, including the recording of unauthorized or non-existent transactions, or inaccurate recording of transactions. Particular risks may arise where multiple users access a common database;
   - The possibility of IT personnel gaining access privileges beyond those necessary to perform their assigned duties thereby breaking down segregation of duties;
   - Unauthorized changes to data in master files;
   - Unauthorized changes to systems or programs;
   - Failure to make necessary changes to systems or programs;
   - Inappropriate manual intervention; and
   - Potential loss of data or inability to access data as required.

(IAASB, 2014 ISA315 (Revised): para. A63)

4. The external auditor is to consider certain situations where reviewing manual internal controls may be less suitable than reviewing the IT controls which include circumstances where:
   - High volume or recurring transactions, or in situations where errors that can be anticipated or predicted can be prevented, or detected and corrected, by control parameters that are automated.
   - Control activities where the specific ways to perform the control can be adequately designed and automated.

(IAASB, 2014 ISA315 (Revised): para. A65)

5. The external auditor is required to understand those control activities that the entity uses to respond to their risks arising from IT (IAASB, 2014 ISA315 (Revised): para. 21). These control activities are considered effective when they maintain the integrity of information and the security of data achieving the specific control objectives of completeness, validity, accuracy and data integrity. The connected explanatory material for this paragraph expands these control activities to include general IT controls as well as application IT controls (IAASB, 2014 ISA315 (Revised): para A103-105). However, no further guidance is given as to what control areas general IT controls and application IT controls cover or a general approach that the external auditor can apply in understanding those controls.

3.13.2.3. Assessing audit risk and developing an audit approach

Using the understanding of the entity, including internal control, the external auditor assesses the risk of material misstatement by considering the likelihood and significance of each of the inherent and control risks identified. The control risk element of the risk of significant misstatement is further driven by the individual internal controls that have been identified as being relevant to the audit (3.11.2.2), which are those internal controls that achieve the control objectives of validity, accuracy and completeness and have been designed effectively. The ISA considers that the control objectives need to be specifically applied to IT related activities and over and above the control objectives that the external auditor considers being completeness, accuracy and validity highlighted in internal control within business governance, the ISA have further expanded on the control objectives in relation to IT to specifically include integrity of data and the security of data (IAASB, 2014 ISA315 (Revised): para. A103). These control objectives and these have been supported by not only by the ISACA glossary of terms (ISACA, 2014) that defines control objectives but by additional research conducted by Julisch *et al.* (2011) in this area.

The ISACA glossary of terms (ISACA, 2014) presents the control objectives specific to IT governance as:

- Completeness: that all information entered into, stored and processed by the information systems of the organisation is complete.
- Accuracy: that information inputs are accurate and that accurate outputs or reports are provided by the information systems after processing.
- Validity: that only valid information is inputted onto the system, only valid changes are made to the system and that no unauthorised access has occurred.

- Integrity: the property that data meet with a priority expectation of quality and that the data can be relied on (Tuttle & Vandervelde, 2007).

Specifically when assessing the integrity of data it implies that no unauthorised changes have been made to the data and that the data has not been corrupted. ISACA further defines data security controls as those controls that seek to maintain confidentiality, integrity and availability of information (ISACA, 2014). To support the requirement that no unauthorised changes have been made to data or unauthorised processing has occurred, the control objective regarding the validity is considered. Achieving this objective will ensure that only authorised individuals have access to approved tasks, elements and data on the IT system. Killmeyer (2006) and Julisch *et al.* (2011) have named this as a separate objective being restricted access, however it is generally accepted to form part of the validity control objective.

Modern business is plagued with an increased risk of cyber security breaches as well as increase legislative requirements regarding the protection of personal information which may result in reputational and financial damage (COSO, 2015; Center for Audit Quality, 2014). These key requirements strengthen the requirement to include the control objective of relating to integrity of data and access or security of all elements of the IT system set out by the ISA as required by the validity control objective.

Using the control objectives of validity, accuracy, completeness and integrity the external auditor will assess which general and application IT controls are a relevant to the audit and this will then determine the nature (test of controls or substantive procedures), proposed timing and extent of planned audit procedures. If in understanding the internal controls of the auditee the external auditor has identified that the relevant IT related controls that are designed effectively and achieve a control objective they will include testing those controls in the planned audit approach.

3.13.3. *Execution (Performing the planned audit procedures)*

The execution phase of the audit process is driven by the audit approach that is created upon completion of the risk assessment procedures in the planning phase. There is a direct link between control risk assessed, regarding both manual and automated controls, in the planning phase of the audit and the test of controls performed in the execution phase of the audit. Each of the IT related controls that were identified as relevant to the audit in the planning phase of the audit will be included in test of controls to verify if the control has been operating effectively throughout the period under review. In the execution phase of the audit the external auditor makes use of several techniques and tools in performing audit procedures.

One of these tools is CAAT's in the performance of both test of controls, through the use of system CAAT's, and as well as substantive procedures, through the use of data CAAT's (Von Wielligh *et al*., 2014; Boynton & Raymond, 2006).

3.13.4. *Reporting (Evaluating the audit evidence)*

The reporting phase of the audit process entails forming the audit opinion and communicating key areas identified in the audit with the relevant stakeholders of the audit. The most recent development in audit reporting is the introduction of paragraphs within the audit report regarding Key Audit Matters for year ends ending on or after 15 December 2016. ISA 701 (revised) paragraph 8 requires the external auditor to communicate those matters that were of most significance in the audit of the financial statements in the current period in the audit report (Cordo & Fülöp, 2015; Christensen, Glover, & Wolfe, 2014). ISA 701 (Revised) paragraph 9 requires the external auditor to consider matters that were communicated with those charged with governance and required significant auditor attention when performing the audit in his/her judgement of significant matters (IAASB, 2014 ISA701 (Revised):para. 8 & 9). Considerations to identify key matters include the following:

1. Areas of higher assessed material misstatement or significant risks identified in terms of ISA 315;
2. Significant auditor judgements relating to areas in the financial statements that involved significant management judgement including accounting estimates that were made in areas of the financial statements; and
3. The audit of significant events or transactions that occurred during the period.

If IT has had a pervasive impact on all areas of the modern business and then the external audit thereof, it can be questioned at what point IT governance at the auditee will be significant enough for its inclusion in the key audit matters section of the audit report. This remains a matter of professional judgement which should take into account:

1. The amount of audit attention given to IT governance throughout the audit, including the need for an expert/specialist;
2. The clear link between the IT system and control risk in the areas where a higher assessment of material misstatement is assessed and significant control deficiencies have been identified; and
3. Significant events or transactions that have occurred in the financial year which include a change in the IT system or key elements of the IT system (IAASB, 2014 ISA710:para. A18 & A29).

The inherent and pervasive impact that IT governance has on the organisation and the external audit of the financial statements may be an indicator that IT governance needs to be given consideration when deciding on what key audit matters to be included in the audit report are.

3.13.5. *Need for additional guidance and evolving audit approaches*

When considering the requirements in the ISA regarding the impact of IT on each of the phases of the audit process, there appears to be sufficient guidance on the pre-engagement and reporting phases of the audit process. However, the impact of IT on understanding the entity's internal control, together with the effect it has on the control risk assessment and planned audit approach at the conclusion of the planning phase and the test of IT controls in the execution phase will suffice in enabling the external auditor to perform the audit without additional guidance to the ISA. It is therefore necessary to investigate what additional guidance is available to the external auditor, who is in the small and medium practice and may not have access to firm specific frameworks regarding the impact of IT on an auditee. The first part of the findings to this study, set out in chapter 4, identify the additional guidance that is currently available to assist the external auditor in assessing the impact of IT on understanding the internal control of an auditee. The fact that the additional guidance is available to the external auditor in understanding IT related controls indicates that external audit has already evolved to account for the impact that IT has had on business and the governance thereof. However in recent years there have been significant developments in control frameworks for IT and there have not been similar advancements for external audit when considering IT. Thus, one needs to consider if the advancement of the audit approach, regarding IT of an auditee, has maintained the pace at which not only IT has evolved, but also how entities are governing IT to ensure that the external auditor appropriately addresses the risks of material misstatement (3.12) as a result of IT within auditee at a strategic and operational or technology level (Center for Audit Quality, 2014; Byrnes & Mcquilken, 2012; Janvrin *et al*., 2008; Yang, 2004).

CHAPTER 4: FINDINGS

4.1. Overview of the findings

The findings of the literature review (Chapter 3) identified a need for additional guidance to the ISA to assist the external auditor when assessing IT related internal controls in the planning and execution phase of the audit process. The research investigated what additional guidance is available to the external auditor of the small and medium sized practice, who does not have access to a firm specific framework, to address IT within an auditee. Using the additional guidance found together with ISA requirements the study assessed if these requirement have evolved in line with advancements in IT and the related IT internal control frameworks. This was done by considering if the ISA and supporting guidance addressed all of the control areas that management would consider when implementing a control framework to govern IT at a strategic as well as an operational level. This assessment identified that there are internal control areas that are included in the IT internal control frameworks that management are using to govern IT that the external auditor, of a small and medium firm, may not be considering when assessing the IT controls of an auditee. To address these areas the author used the current approach that the external auditor applies in identifying controls that are relevant to the audit as the basis to recommend a comprehensive approach to address IT related controls of an auditee.

4.2. Additional guidance to support ISA

As explained in the literature review (Chapter 3) the external auditor requires additional guidance when assessing the impact of IT on an auditee in the planning phase of the audit process, specifically when understanding the entity and its internal control. The ISA, in ISA 315, highlights specific considerations that the external auditor needs to apply regarding IT when understanding the impact of IT within an auditees broader internal control framework. Similar to the manner in which COSO gives the external auditor a high level overview of how to understand the entity's internal control, the ISA provides broad guidance requiring the external auditor to assess IT controls, the benefits and risks of IT, if any IT controls will impact the risk of material misstatement and the general and application IT controls of an auditee. In order for the external auditor to identify the controls that are relevant to the audit, and which achieve control objectives thereby reducing control risk, the external auditor requires more detailed guidance of what control areas are included in general and application controls.

Von Wielligh *et al.* (2014), Marx *et al.* (2014), Boynton & Raymond (2006) and Arens and Loebbecke (1980) have over time categorised and explained the general and application IT controls into control areas to assist the external auditor in identifying IT controls that are relevant to the audit by assessing the design of and testing the operating effectiveness of these explained IT controls (Singleton, 2010). The internal control areas presented by these authors overlap and address similar areas of focus despite the time-lapse between them. For this reason a single summation of the control areas was selected to understand how the external auditor, using the ISA, currently assesses internal control activities within the general and application controls relating to IT. The detailed control areas highlighted by Von Wielligh *et al.* (2014) were selected to be the basis from which to understand and expand on the control areas within the general and application IT controls, however, any of the supporting texts will reference the majority of the control areas.

4.2.1. General IT controls

General IT controls are those policies and procedures that relate to all the applications used by the IT systems and support the effective functioning of all applications (Julisch *et al.*, 2011). These include oversight controls and then key areas of the IT environment such as data centre and network operations, system acquisition, change and maintenance, program change, access security and application system acquisition, change and maintenance (Rubino & Vitolla, 2014; IAASB, 2014 ISA315 (Revised): para. A103-A105; Von Wielligh *et al.*, 2014; Marx et al., 2014; Huang *et al.*, 2011; Gheorghe, 2010; Boynton & Raymond, 2006; Yang, 2004; Siyana, 2002; Arens & Loebbecke, 1980).

If the external auditor chooses to use any part of, or output from the IT system, including printouts, he/she will need to assess the general IT controls of the entity. Given the complex and integrated nature of IT in business today it is unlikely that there will be many instances where this is not the case (Singleton, 2010). For this purpose, the brief areas included in general IT controls in ISA315 have been described by Von Wielligh *et al.* (2014), Marx *et al.* (2014), Boynton & Raymond (2006) and Arens and Loebbecke (1980) to include:

- **Organisational controls and personnel practices:** Internal controls relating to the corporate structure, responsibility levels and reporting lines relating to IT governance. The role of the Computer Steering Committee and Chief Information officer at a strategic level as well as all other IT personnel are included. The reporting lines, supervision and review of all IT personnel as well as best practices for hiring, retaining, performance managing and if necessary dismissing IT personnel.

- **System development and acquisition controls:** Internal controls relating to the acquisition or in-house development of a new IT system, this usually entails a large project and marks a significant change to the IT system of the entity. Internal controls will address the request, needs assessment and approval; planning and project management of the change and design of the new IT system in line with the policy and standards in place; systems development and testing; implementation and post implementation review.
- **Program change controls:** Internal controls relating to the change of an IT software program already in use by the organisation to enhance program performance and address changing user needs, this is usually a small project and will not necessarily have a significant impact on the IT system as a whole of the entity. Internal controls will address the request, needs assessment and approval; planning and project management of the change and design of the changed program in line with the policy and standards in place; systems development and testing; implementation and post implementation review.
- **Access controls:** Internal controls relating to physical and logical access to IT facilities, personnel, hardware and software, specifically including data. These internal controls include preventative controls such as physical security, logical authorisation matrices and passwords as well as detective controls such as reviewing of physical and digital access logs.
- **Business continuity controls:** Internal controls which ensure the continuity of IT operations in the event of a major or minor disruption. These controls include preventative controls such as protection against physical dangers such as fire, water and environmental changes and non-physical dangers such as unauthorised access to the system to disrupt IT operations. These internal controls also include corrective controls in the event of a disruption such as a disaster recovery plan and back-up procedures.
- **Operating controls and system maintenance:** Internal controls that relate to the operating of the IT system including the use of assets, scheduling of processing and other IT related tasks, the librarian function and reviewing of operating logs. System maintenance in this context does not include running of maintenance upgrades to hardware and software, but rather focusses on the effective operating of the IT system as a whole.

4.2.2. Application IT controls

Application IT controls are those controls (manual or automated) that usually operate at a business process level that apply to processing of transactions by individual applications (IAASB, 2014 ISA315 (Revised): para. A103-A105). Application IT controls are dependent upon the operating effectiveness of the general IT controls and can only be considered in an external audit when the general IT controls are operating effectively. Presently, the external auditor focusses on the application controls that relate to applications used in the financial reporting systems to avoid material misstatement (Center for Audit Quality, 2014). Application IT controls are classified as input controls, processing controls, output controls and master file amendment controls within the IT system of the entity (Runino & Vitolla, 2014; Chang *et al*.., 2014; Von Wielligh *et al*., 2014; Marx *et al*., 2014; Boynton & Raymond, 2006; Flowerday & Von Solms, 2005; Sayana, 2002; Arens & Loebbecke, 1980). These have been explained by Von Wielligh *et al.* (2014), Marx *et al*. (2014), Boynton & Raymond (2006) and Arens and Loebbecke (1980) as:

- **Input controls:** Internal control activities relating to recording of data on documents, capturing of data onto the IT system, error identification and correction in the input process and review and investigation, if necessary, of electronic logs regarding input.
- **Processing controls**: Internal control activities surrounding the accurate processing of information within applications including using the correct version of the program, use of control totals whilst processing, programmed validation tests within applications, processing error identification and correction as well as the review and investigation, if necessary, of electronic logs regarding processing.
- **Output controls:** Internal control activities surrounding the correctness of output generation by the application, appropriate distribution of output and output error identification, correction as well as review and investigation, if necessary, of electronic logs regarding output.
- **Masterfile amendments controls:** Internal control activities surrounding the documentation of authorised amendments to Masterfile's, capturing of authorised amendments onto master files, input error identification and correction and review and investigation, if necessary, of electronic logs and financial data relating to master file changes.

As the external auditors assessment of the IT controls is dependent upon the internal control framework that is selected by management. If IT Governance, as required by King III, spans the entire spectrum of the organisation from a strategic point of view down to the individual hardware and software components used every day in the entity then the external auditor will also need to consider this entire spectrum of controls.

Recent advancements in IT that have directly impacted all businesses, no matter the size, for example “Bring Your Own Device”, automated online processes and integration of IT with production and supply chain processes, need to be accounted for in the entity’s IT governance approach and consequently the external auditors understanding thereof. It is doubtful if the external auditor, in the small and medium practice, without access to firm specific IT frameworks, will solely through the consideration of general and application IT controls explained above, address all of the control areas, strategic and operational or technological, as well as address the related control risks of material misstatement that arise as a result of the use of IT in the auditee. The research investigates whether the general and application IT control areas, that the external auditor within the small and medium practice applies in the performance of the external audit, have kept pace with advancements in IT, that have effected all businesses, and the supporting IT control frameworks to address the risk of material misstatement.

4.3. Insufficient guidance in the ISA to address the evolution of IT and the frameworks to govern IT of an auditee

The external auditors understanding of the auditee’s internal control is based on the internal control frameworks that have been selected by management to achieve their control objectives. IT Governance, as required by King III, spans the entire spectrum of the organisation from a strategic point of view down to the individual hardware and software components used every day in the entity. IT governance frameworks are available to assist management of the entity to achieve IT governance. The control areas highlighted by Goosen and Rudman (2013) in the “*Integrated Framework*” will assist management to govern IT at a strategic as well as an operational or technology level in the wake of evolving IT (3.7). The research investigates whether control areas identified within the control activities as required by the ISA, and supporting guidance, relating to general and application IT controls provide a comprehensive approach to assess IT governance. To do so, a comparison was performed between the general and application IT controls areas explained in ISA 315, together with the expanded guidance provided by the audit experts such as Von Wielligh *et al.* (2014), Marx *et al*. (2014), Boynton and Raymond (2006) and Arens and Loebbecke (1980), with the strategic and operational or technology level control areas identified by Goosen and Rudman (2013). The complete comparison is presented in Appendix 1 at a strategic or general control level and Appendix 2 at application control and operational or technology level. Appendix 1 shows that through comparing the internal control areas in the ISA at a strategic level to the control areas in the integrated framework using the current general IT control areas the external auditor will address all of the IT risks at a strategic level.

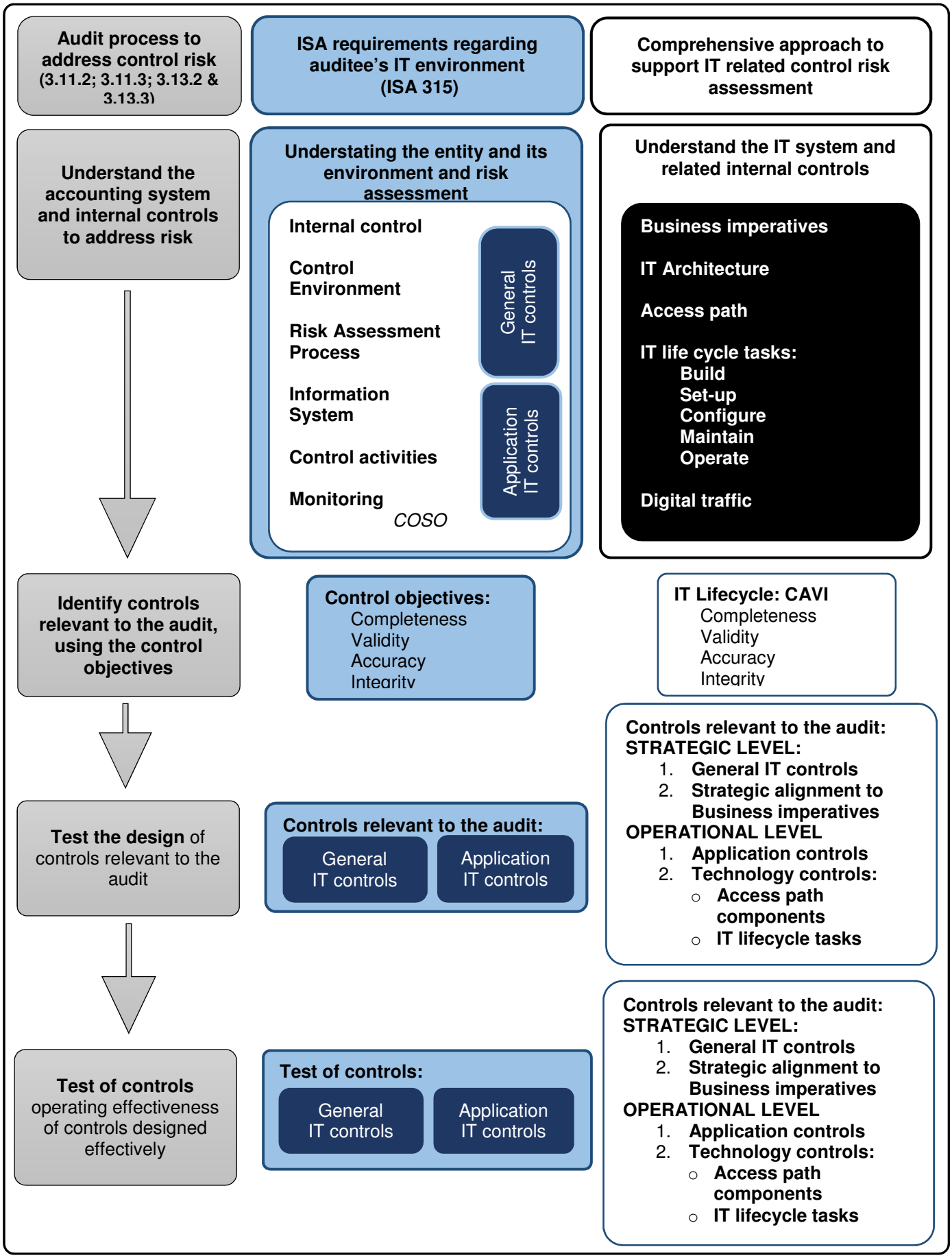
Appendix 2 however, shows that when comparing the operational or technology level control areas there are in fact some areas at a technology level that are not addressed by the external auditor when considering the application IT control areas. The application control areas only address certain of the components of the access path (3.7) and for those components of the access path addressed only certain of the IT life cycle tasks are addressed (3.7). The reason for this gap is that the scope of the external auditor's application IT control assessment is generally limited to individual applications that have a direct impact on financial reporting (Center for Audit Quality, 2015). It thus excludes other hardware and software of the specific application and its underlying data that may expose the organisation to additional risks of material misstatement through not achieving the control objectives. Further, the evolution of IT and its pervasiveness have heightened the risk and focus on cyber security within the entire IT system and present a very real threat for organisations today and supports the need to increase the external auditor's scope over more components of the IT system (Center for Audit Quality, 2014; IODSA, 2009; IODSA, 2016). This confirms the need to increase the scope of the external auditor's assessment of IT controls of an auditee, this also impacts the risk of material misstatement of a larger number of hardware and software components in the IT system.

In order for the external auditor of the small and medium practice, who does not have access to firm specific frameworks, to address all the risks of material misstatement that arise as a result of IT governance within an auditee, a comprehensive approach is needed. The next section presents a proposed comprehensive approach that the external auditor of the small and medium practice can use to address these IT risks of material misstatement.

4.4. A comprehensive approach to address the risk of material misstatement that arise from IT

Due to the deficiencies in the ISA, together with the supporting guidance, that the external auditor of the small and medium firm has at his/her disposal, a comprehensive approach has been developed to ensure that control risk is assessed comprehensively within an auditee, including the risk exposure at a technology level, in conjunction with the current general and application IT controls. Figure 1 highlights the process followed to develop the comprehensive approach and comprises of three sections.

Figure 1 Overview: Comprehensive approach to assist the external auditor, in the small and medium firm, in understanding and assessing IT related control risk



The first section represents the process that the external auditor follows when identifying which internal controls are relevant to the audit and if reliance can be placed on the internal controls in assessing control risk. This process includes obtaining an understanding of the accounting and internal control system (3.11.2.2), identifying internal controls relevant to the audit, or key controls, which will achieve the control objectives (3.11.2.2), testing the design of the key controls, to identify if the key controls are designed in such a manner that they will achieve the control objectives (3.11.2.3) and finally to test the operating effectiveness of the key controls throughout the financial period under review (3.11.3).

The second section of Figure 1 expands the basic approach, in section 1 of Figure 1, with the relevant ISA, and supporting guidance (specifically relating to IT). This guidance is based on the consideration of the elements of COSO (3.11.2.2) which are used to understand the accounting system and internal controls, both manual and automated, of the auditee. The relevant control objectives relating to IT that are used to identify key IT controls are completeness, validity, accuracy and data integrity (3.13.2.3). Finally, the ISA, together with the supporting guidance, use the general and application IT controls as the basis to test the design of and operating effectiveness (test of controls) of the key IT related internal controls that are relevant to the audit.

This study found that the general and application IT controls alone do not suffice in addressing all of the IT related control areas and risks that are present at an auditee (4.3). In order to address this, the comprehensive approach to support IT related control risk, shown in the third section of Figure 1, was developed. Firstly, the study investigated how a complete understanding can be obtained of the impact of IT on the entity and its control environment by considering the elements of COSO and how, IT impacts each of these elements. This showed that the elements of IT governance consisting of business imperatives, IT architecture, access path, IT life cycle tasks and digital traffic can be used as a comprehensive basis to understand IT related internal controls. The IT life cycle tasks (3.7) can then be used, together with the control objectives, to identify key IT related internal controls key controls that are relevant to the audit, over and above the general and application IT controls that have already been identified as being relevant to the audit. The design of the key IT controls that are at are relevant to the audit are shown at a strategic and operational level in comprehensive approach (third section of Figure 1). And finally, for those key IT controls that have been assessed as designed effectively, the operating effectiveness will also need to be tested at a strategic and operational level in order for the external auditor to make his/her final assessment of control risk and ultimately the level of detection risk that he/she is willing to accept.

4.4.1. Business Governance and IT Governance

In order to develop a comprehensive approach to ensure that the external auditor of the small and medium firm, identifies all of the IT related internal controls that are relevant to the audit a link needs to be drawn between the areas that the external auditor considers to understand the auditee and its environment, using COSO and the requirements in the ISA (3.11.2.1 and 3.11.2.2), and the IT impact on each of these areas. Boshoff (2104) provided a framework to do this. Table 1 shows the elements of business governance and the elements of IT governance. Before the IT governance areas (Panel 2 in Table 1) can be used within the comprehensive approach, it must first be considered if all the necessary areas of COSO and the ISA are included within business governance (Panel 1 in Table 1).

Table 1: Business Governance and IT Governance

Panel 1: Business Governance	Panel 2: IT Governance
Business Model	Business Imperatives
Business Process	IT Architecture
Workflow	Access Path
Internal Control – CAV	IT Life cycle – CAVI
Manual tasks and Procedures	IT Life cycle tasks
Discrete automated procedures	Digital traffic

A detailed explanation of each of the elements of business governance (Panel 1 in Table 1) is described in the following section. After each element of business governance is discussed, a box in italics is included to explain the manner in which the external auditor currently considers the specific element of business governance when understanding the auditee and its environment to and identifying key internal controls that are relevant to the audit.

4.4.2. Business Governance

The elements included in business governance (Panel 1 in Table 1) suggest a comprehensive approach to ensure that leadership of the organisation are using the business model to drive how the business is run including the internal controls that are implemented within in each area of the business by using a top down approach and aligning each of business governance to the element before (Boshoff, 2014).These elements are discussed below.

4.4.2.1. Business Governance - Business Model

Each business finds itself in a unique internal and external context that impacts how that specific business is operated at a strategic and operational level. A strategic overview of the business needs to be created that explains this internal and external context, in the form of a business model. Teece (2010) claims that the essence of a business model is the unique way that an organisation delivers value to customers, entices customers to pay for value, and converts those payments to profit. Teece (2010) further explains the business model as a conceptual rather than financial model of a business. An entity's business model is framed within the global, local, industry and maturity scale of the specific entity and will be unique, even where entities find themselves in the same local and industry context (Boshoff, 2014; Baden-Fuller & Morgan, 2010). The term business model is synonymous with and supports the idea of an organisation's strategy and is driven by the leadership of the organisation (Baden-Fuller & Morgan, 2010).

Osterwalder and Pigneur (2010), in the book Business Model Generation, use the business model canvas to identify key areas that an entity's business model will require to effectively support the organisation to success. These areas include value propositions, key partners, key activities, key resources, customer relationships, channels, customer segments, cost structure and revenue streams. The business model thus highlights the entity specific focus areas which then drives how the entity operates in order to achieve the vision and strategy. The business model is supported by certain basic business assumptions, applicable to any entity, for example profit orientation, cash flows and support structures that are not necessarily highlighted in the business model. The business model has a direct impact on how the business is governed and should thus drive how IT is governed.

In understanding the entity and its environment the external auditor will need to understand the auditee's business model as part of placing the entity into context (3.11.2.1).

4.4.2.2. Business Governance - Business Processes

The business model of the entity must to be expanded upon to give the entity clear guidelines on how to operate through the use of business processes. Business processes are a set of activities that are performed in co-ordination in an organisational and technical environment (Vasarhelyi & Romero, 2014; Weske, 2010). These co-ordinated activities across business processes jointly achieve the organisations goals. They stem directly from the business model and will be widely structured around the organisation's goals and strategies.

From a financial reporting view point these business processes have been broken down into specific cycles including revenue, purchases, inventory, human resources and financing and investment (Marx *et al*., 2014; Von Wielligh *et al*., 2014). Business processes are interlinked and the entity will require an overview of how each of the business processes links into each other in the operation of the entity. Each business process can be broken down into tasks that are performed at each stage of the business process, these are explained in Business Governance – Work flow below (4.4.2.3). In a modern business, it is more than likely that IT will be integral to and support business processes. Just as the business processes set a broad map of how each of the areas in a business overlap the IT architecture, it will amongst other areas, show how IT is integrated to and supports the business processes.

In understanding the internal controls of the entity, the external auditor will first need to understand the business process before he can obtain understanding of the internal controls that have been applied to each business process (3.11.2.2).

4.4.2.3. Business Governance – Work flow

Business processes are the broad categories within which transactions or events are grouped based on the nature of the event. This is then further expanded into a workflow. The Oxford English Dictionary defines a workflow as a noun:

> *"The sequence of industrial, administrative, or other processes through which a piece of work passes from initiation to completion; the passage of a piece of work through this sequence."* (Oxford English Dictionery, 2014, s.v. 'workflow')

Workflows give the overview of the tasks included within each individual functional or transactional process of the business (Von Wielligh *et al*., 2014). This implies that when understanding the entity and its environment, the external auditor needs to understand the detail of the business processes, and the tasks therein, and how events or transactions that occur, move through the accounting process to be presented in the financial statements of the entity. The accounting process, which in essence is a workflow, considers how each event within a particular business process is initiated, executed, recorded, processed and reported (Marx *et al*., 2014; Von Wielligh *et al*., 2014). Throughout the workflow tasks and internal controls, manual or automated, are implemented by management to ensure that the control objectives are met.

In understanding the internal controls of the entity, the external auditor will further need to understand how the business process are explained in workflows before he can obtain understanding of the internal controls that have been applied to each business process (3.11.2.2).

4.4.2.4. Business Governance - Internal control – CAV

Within each business process, management is required to implement a system/framework of internal control that will address specific control objectives and support management in asserting that the financial statements are correct (IODSA, 2009). The business processes that represent the operations of the entity and ultimately the information included in the financial statements will need to ensure that at each point there are internal controls to ensure that the information outputted from the business processes is correct. COSO (3.6) is a commonly used internal control framework to support management's assertions over the financial statements. COSO includes specific control objectives that need to be achieved to enable the management to assert that the financial statements, and the information included therein are correct. The broad control objectives that need to be addressed based on COSO, discussed in section 3.6, are the efficiency and effectiveness of operations, reliability of financial reporting and compliance with applicable laws and regulations (Rubino & Vitolla, 2014; COSO, 2013). These broad control objectives are not in sufficient detail to aid the external auditor in his understanding and risk assessment of the entity and its business processes at an operational level without being expanded upon. Specifically regarding the reliability of financial reporting in the form of control objectives being completeness, accuracy and validity *(3.11.2.2).*

Management needs to design and implement internal controls, through manual or automated activities, within each business process and its related workflow tasks explained above, that will ensure that each of the control objectives are achieved at each stage of the workflow and ultimately result in the information included in the financial statements. If the IT architecture is integral to and supportive of the business processes, then the control objectives to be achieved on manual elements of the workflow will also need to be achieved by their automated counterparts.

The external auditor clearly needs to understand the control objectives to assist him/her in identifying which controls are relevant to the audit by assessing if the internal controls included in the manual tasks and procedures and the discrete automated procedures achieve the control objectives (3.11.2.2).

4.4.2.5. Business Governance – Manual tasks and procedures

Within each workflow at each stage in the accounting process, specific activities or tasks take place to ensure that the control objectives are met. These activities directly link to the control activities set out in the COSO model and include segregation of duties, performance reviews, Information processing, physical controls and approvals (COSO, 2013).

The external auditor clearly needs to understand how the manual tasks of procedures achieve the control objectives to assist him/her in identifying which controls are relevant to the audit (3.11.2.2).

4.4.2.6. Business Governance – Discrete automated procedures

Certain of the control activities are implemented through the use of discrete (individual or separate) automated procedures within an IT application in business governance. These procedures will achieve a similar result to their manual counterpart; however they are programmed within the IT application that is used by the organisation. These discrete automated procedures will be documented within the workflow of the entity and need to be clearly understood by management as well as the external auditor when assessing business processes, workflows and internal controls to meet the control objectives.

The external auditor clearly needs to understand how the manual tasks of procedures achieve the control objectives to assist him/her in identifying which controls are relevant to the audit (3.11.2.2).

4.4.2.7. Each of the elements of COSO are represented within business governance

The above discussion shows that when the external auditor is understanding the entity and its environment (including internal control) giving consideration to each of the elements of COSO, each of the elements of business governance (Panel 1 in Table 1) are being addressed. To enable the external auditor to fully address the requirements of the ISA in understanding the entity (including internal controls both manual and automated) the external auditor first needs to clearly understand business governance as well as its IT governance equivalent element (Panel 2 of Table 1). The elements of IT governance may be considered to be an appropriate basis to use in the comprehensive approach.

However, as the external auditors understanding of the auditee is based on the internal controls that have been implemented by management, the author first considered if the areas included in IT governance (Panel 2 in Table 1) will enable management to govern IT comprehensively. To do so the elements of IT governance (Panel 2 of Table1) were compared to the control areas identified by Goosen and Rudman (2013) (3.7). The results of this comparison are set out in Appendix 3 and show that by using the elements included in IT governance management will have a comprehensive approach to govern IT as it addresses all of the control areas identified by Goosen and Rudman (2013). Consequently. as the elements of IT governance (Panel 2 in Table 1) provide management with a comprehensive approach to govern IT and can be linked to all of the areas that the external auditor needs to consider, through the business governance elements (Panel 1 in Table 1), when understanding the entity and identifying key internal controls that are relevant to the audit, the elements of IT governance (Panel 2 in Table 1) are the base for the comprehensive approach.

4.4.3. IT Governance

Each element of IT governance (Panel 1 in Table 1) is explained in the following paragraphs, thereafter the external auditor of the small and medium firm's application of each element of IT governance within the comprehensive approach follows in section 4.4.4.

4.4.3.1. IT Governance - Business imperatives

From the business model, the entity must identify certain strategic objectives that those key priorities and specific battlegrounds that if addressed correctly will ensure the specific organisations competitive edge an*d* ultimate success and if not the organisations demise, these are business imperatives. Business imperatives as is the case with the business model are supported by the basic business assumptions. Business imperatives are directly influenced by the specific entity's internal and external context including vision and strategy, industry, geography, market segment and size which will also have been the foundation for the business model (Boshoff, 2014; Goosen & Rudman, 2013; Gheorghe, 2010).

Each business imperative will have a direct impact on the IT architectures the entity will require and what the entity requires IT to deliver to support it in achieving the business imperatives (Boshoff, 2014; Gheorghe, 2010). Business imperatives are the foundation for achieving IT alignment with the business strategy that is required by King III and have proven to be a key in entity's that perform well (Coltman, Tallon, Sharma & Queiroz, 2015; Gerow, Thatcher & Grover, 2015; IODSA, 2009).

Management is required to create and document business imperatives in alignment with the business model as well as how business imperatives are achieved in the IT architecture implemented by the entity, which is assessed on a regular bases by the leadership of the organisation (IODSA, 2009).

4.4.3.2. IT Governance - IT Architecture

Information technology architecture is the alignment between the business imperatives that stem from the business models and business processes and the IT applications, IT infrastructure and data required to achieve the business imperatives. IT architecture is unique to each organisation and fits into and supports the business processes of the entity, whilst specifically addressing the business imperatives identified by management of the entity. IT architecture is a written and/or graphic plan that sets out the overall high level structure of the organisation's information system and then breaks it down into individual elements referred to as domains.

The IT architecture sets out the individual hardware, software, network and other components required for that domain to function effectively and it further documents how each domain of the information system interacts or connects with other elements domains thereof (Boshoff, 2014; ISO, 2011; Op't Land, Proper, Waage, Cloo & Steghuis. 2009; Emery & Hilliard, 2009). The IT architecture will further provide an overview of the access paths within the IT system as explained in 3.7.

4.4.3.3. IT Governance - Access Path

The access path is the path a user takes to perform computerised activities (Boshoff, 1990) (3.7). Should management of the entity use IT in the execution of workflows or in financial recording and reporting to ensure that the control objectives are achieved by the system of internal control, management will need to ensure that internal controls are applied to and within each component of the access path through the use of the IT Life Cycle tasks or configuration controls (Boshoff, 2014; Goosen & Rudman, 2013; Killmeyer, 2006) (3.7).

4.4.3.4. IT Governance – IT life cycle: CAVI

The IT architecture that is implemented, through the IT Lifecycle, tasks to support the business processes and correlating internal control frameworks adopted by the entity will need to achieve the internal control objectives (Von Wielligh *et al*., 2014). These control objectives are completeness, validity, accuracy and integrity as discussed in 3.13.2.3.

4.4.3.5. IT Governance – IT Life cycle tasks

The IT Life cycle tasks are the technology level internal controls that are implemented for each component of the access path that include how the component is built, set-up, configured, maintained or operated (3.7).

4.4.3.6. IT Governance - Digital traffic

At the base of any IT architecture is the flow of digital traffic amongst hardware, software and across networks. Digital describes the technology used by computers to generate, store and process data in binary code form of "0's" and "1's" (Beal, 2016b, s.v. 'digital'; Electronics glossary Whatis.com, 2005, s.v. 'digital'). Traffic in the IT sense is defined by Webopedia (2016, s.v. 'traffic') as the load on a communication's device or system. Digital traffic is not part of the access path; however, it will move through each of the elements of the access path as part of the functioning of the IT system. From an IT governance point of view to control the flow of digital traffic outside, and even to an extent, inside of the hardware and software elements of the IT system is nearly impossible. Management will thus have to ensure that appropriate internal controls have been around each of the components of the access path as well as each of the IT life cycle tasks for the access path component to address and govern digital traffic.

Using all of the above elements of IT governance (Panel 2 in Table 1) management will have a comprehensive approach to govern IT within the business, which aligns to business governance (Panel 1 in Table 1). Similarly, using the elements of IT governance from Panel 2 in Table 1 as the basis for the extended approach (third section in Figure 1), together with the current general and application IT controls, will provide the external auditor with a comprehensive approach to address IT risks of material misstatement and the related internal controls within an auditee.

4.4.4. Applying proposed extended approach when considering IT governance and the related control risk of an auditee

In performing the external audit, the auditor of the small and medium practice, already considers the general and application IT controls that exist within the auditee. In reviewing the general IT controls the basic assumptions to the effective functioning of the IT processes within the auditee are assessed through the effective functioning of the IT General controls (4.2.1 and Appendix 1). Further, by addressing the application IT controls, the input, processing, output and master file changes relating to the financial application and supporting processes are reviewed.

However, this leaves the risks that present themselves as a result of the type of IT architecture that the auditee implements in line with the business imperatives and does not take into account each of the potential access paths to the IT systems of the auditee. To address these risks, the elements of IT Governance form the basis for the comprehensive approach (third section in Figure 1). However, digital traffic, as the only area of IT governance that is not within the entity's control and to which internal controls cannot be applied by management, it is not considered by the external auditor in execution of the comprehensive approach.

The considerations of the external auditor within each of the remaining elements of IT governance is described in the sequence that the external auditor would consider them in applying the comprehensive approach.

4.4.4.1. IT Governance - Business imperatives

The external auditor will need to understand the business imperatives that management have identified and ensure that they align to the business model of the entity and then directly flow through to the IT architecture, this is performed as part of the external auditors process of understanding the entity and its environment (3.13.2.1).

4.4.4.2. IT Governance - IT Architecture and Access paths

As part of understanding the entity and its internal control (3.13.2.2) the entity specific IT architecture will give an overview of what technologies, hardware and software are used by the entity and will identify each user who performs computerised activities within the entity. These will identify the access path and the components therein for the IT system. For the financial IT application and underlying data the IT architecture will at a minimum show that not only the finance personnel but also that IT personnel have access (Gantz, 2014). If the IT system increases in complexity in line with business imperatives it could, for example include online real time sales personnel and members of staff in various functional areas. Each user identified will have their own access path to the application and underlying data, however, there may be components of each users access path that are shared across all the users access paths. For the external auditor to ensure that each of the control objectives of completeness, validity, accuracy; data integrity and privacy compliance are achieved - each of these identified access paths will need to be understood and assessed. The general auditor in the small and medium firm may not have the necessary expertise to understand the IT architecture or the components of the access paths as they increase in complexity, it is however, still necessary for this exercise to be performed in the planning phase of the audit process and the external auditor may need to consider the use of a specialist to do so.

The specific components of any access path will be as varied in complexity and length as the entity itself, however, there are some components that are common in various IT systems (Gantz, 2014).

For purposes of this study a selection of these common components have been included to illustrate the components of the access path; however, this list is not exhaustive. Further, as access path components are developed and manufactured by varying companies and service providers, a generic explanation of each of the components is included and will need to be supplemented by the manufacturer or developer specifications, these include:

- **User computer (desktop or laptop):** Hardware components that make up a user computer including amongst others the screen, keyboard, processor and hard drive.
- **Mobile device:** A handheld computing device that enables the concept of wireless computing though the use of wireless networks to the internet (ISACA, 2014).
- **Installed device operating software:** Computers, mobile devices and servers require operating systems to drive their functioning and support their computing needs. It is the master control program that interfaces between the hardware and the software, controls access to devices and applications on the computer or mobile device and sets the standards for the applications that can be run on the operating system (ISACA, 2014; Gantz, 2014).
- **Network switch:** A networking device that creates a local area network by connecting IT assets in a network including computers, printers and servers (What is a Network Switch vs. a Router?, 2016; ISACA, 2014).
- **Network router:** A networking device that routes (sends) data packets from one network to another. It links computers to the internet enabling multiple computers on the network to share the same internet connection (What is a Network Switch vs. a Router?, 2016; ISACA, 2014).
- **Firewall:** A piece of hardware or software that acts as a boundary to a network preventing unauthorised access by screening and approving or rejecting requests for access to the network. A firewall can form part of the network router at the entry point to the network (What is a firewall?, 2016; ISACA, 2014).

  Firewalls can be used to create a demilitarised zone (DMZ) within a network and creates a buffer zone between the outside untrusted network and internet and the trusted internal network. This can ensure data and requests from an untrusted source are fist subject to the security protocols of the firewalls to prevent unauthorised or malicious access to the network. The DMZ will be reflected in the IT architecture but will be achieved through the use of firewalls and as such is not viewed as a separate access path component.

- **Asymmetric Digital Subscriber Line (ADSL):** Is a communications technology that allows telephone lines to receive both voice and data at the same time. ADSL services are provided by external service providers to the entity (Beal, 2016a, s.v. 'ADSL').
- **Virtual Private Network (VPN):** Is the extension of a private network over a public network for example the internet, through the use of tunnelling protocol. This is done either by solely adding software to existing hardware or by acquiring hardware with applicable software solely dedicated to efficient running of the VPN. VPN software is installed on both the sending and receiving IT asset to encrypt and decrypt the data that is sent securely across the VPN. VPN services are provided by an external service provider who will provide the software to activate and manage the VPN (ISACA, 2014; Salamone, 2013; How VPN works, 2003).
- **Internet:** The connection of two or more networks by a network router (ISACA, 2014). The organisation itself has no control over the data once it has passed through the network router through the firewall to the internet.
- **Server:** A computer or program in a network that "serves" other (client) computers on the network with shared resources. Client computers request access and execution from the shared resources on the server and the server supplies the requested resource. There may be several servers within a network that may include for example an application server, database server, printer server, email server and web server (ISACA, 2014; Electronics glossary Whatis.com, 2014, s.v. 'server').
- **Server operating software:** When a computer network makes use of a server, specialised software is required on both the server as well as the requesting client computers on the network (ISACA, 2014).
- *Applications:* Application is a program that preforms processing of records for a specific function. Functions can range from recording of accounting transactions, reporting on entity specific operations or financial information to word processing (ISACA, 2014; Gantz, 2014).
- **Data base management system:** Software system that controls the organisation, storage and retrieval of data in the data base (ISACA, 2014).
- **Data base:** A collection of data created, categorised and maintained in an organisation that generally supports more than one application and/or business process and is used to meet the organisations processing and retrieval requirements (ISACA, 2014; Gantz, 2014). The data base is housed on a server as set out in the IT architecture and operated by means of a data base management system (Gantz, 2014).

Once the external auditor has identified each of the components in the access path, he/she will need to understand which of the IT life cycle tasks and the controls surrounding each life cycle task (3.7) are relevant to the component. Only, then will the external auditor consider which control objectives need to be addressed by each of the life cycle tasks to identify which controls are relevant to the audit.

4.4.4.3. IT Governance – IT Life cycle tasks

The IT Life cycle tasks span the entire life cycle of a technological component within an access path from the initial acquisition or in-house development through to maintaining of the component. The nature of the technology of the access path component drives which of the IT Life cycle tasks are relevant to the particular access path component and not all the IT Life cycle tasks are applicable to each access path component. Table 2 identifies which of the IT Life cycle tasks are relevant to each of the common components of the access path

Table 2: IT Life cycle tasks (configuration controls) for relevant components of the access path (3.7)

Common components of an access path per 4.6.3	Hardware or software	Computer hardware build	Computer software build	Setup or installation	Configuration	Operating a computer	Computer maintenance
User computer (desktop or lap top):	Hardware	Maybe[1]	No	Maybe[2]	No	No	Yes
Mobile device	Hardware	No	No	No	No	No	Yes
Computer (desktop or lap top) operating software	Software	No	Maybe[3]	Yes	Yes	Yes[4]	Yes
Installed mobile device operating software	Software	No[5]	No[5]	Yes	Yes	No	Yes
Managed network switch	Hardware and software	No[6]	No[6]	No[6]	Yes[7]	No	Yes[7]
Unmanaged network switch	Hardware	No[6]	No[6]	No[6]	No[7]	No	No[7]
Network router	Hardware and software	No[6]	No[6]	No[6]	Yes	Maybe[8]	Yes
Firewall	Hardware and/or software	No[6]	No[6]	No[6]	Yes	Maybe[8]	Yes
ADSL[9]	Hardware and software	No	No	No	No	No	No
VPN[10]	Hardware and/or software	No	No	Yes[10]	Yes[10]	No	Yes
Server	Hardware	Maybe[1]	No	No	No	No	Yes
Server operating software	Software	No	No	Yes	Yes	Yes	Yes
Applications	Software	No	Maybe[11]	Yes	Yes	Yes[12]	Yes
Data base management system	Software	No	Maybe[11]	Maybe[13]	Yes	Yes	Yes
Data base	Software	No	No	No	Yes	Yes	Yes

Legend follows on next page.

Table 2: IT Life cycle tasks (configuration controls) for components of the access path (3.7)

Legend Table 2:

[1] The user computer (desktop or laptop) as well as the sever may be purchased from a reputable supplier or can be built in-house if the IT capabilities are available.

[2] The user computer (desktop or laptop) as well as the sever may be set up (including all of the programs et cetera required to execute the required operations) prior to receipt of the hardware and related software from the manufacturer; alternatively a member of the IT department may need to set it up and install the required software programs.

[3] The software that is required to operate a user computer is usually provided with the device by the manufacturer; in the case of entity in-house built hardware, the entity may also need to develop the complementing operating software.

[4] Despite having the capabilities to be operated, a user computer with the related software is unlikely to be operated by the majority of users without the technical knowledge to do so.

[5] The hardware of a mobile device as well software required to operate a mobile device is always provided and/or installed by the manufacturer thereof on the mobile device.

[6] Network routers; network switches and firewalls are hardware devices with complementing software that are manufactured by specialists and it is highly unlikely that the organisation will build these pieces of hardware or the complementing software.

[7] A network switch can either be managed or unmanaged. Unmanaged network switches are not designed to be configured and thus are merely "plug-and-play" - no configuration or maintenance is required. A managed switch however, is configurable and maintenance may be required (What is a Network Switch vs. a Router?, 2016).

[8] Network routers and firewalls, which can form part of the router, can be operated when assessing incoming data to the local area network and setting firewall rules of who has access.

[9] ADSL is provided by an external service provider who will perform all of the functions in the IT life cycle for the ADSL line, even set-up and installation will not be required as it will be provided by the external service provider. The selection of a service provider is thus all that is in control of the organisation and will be addressed in the IT general controls.

[10] VPN software may specifically need to be added to existing hardware, for example routers and personal computers, of the organisation. The software will need to be set-up and installed and/or be configured to the organisations specifications. If additional hardware is acquired it may already be set up and merely the initial configuration may need to be done. As an external service provider provides VPN services it is expected that the majority of the functions of the IT life cycle will be performed by them and thus will not be in the control of the organisation. The selection of a service provider is an important decision that is in control of the organisation and will be addressed in the IT general controls.

[11] Applications as well as the data base management system may be developed in-house or purchased depending on the availability of IT resources and products that service the organisations IT architecture requirements.

Legend Table 2 (continued):

[12] The complexity and source of the application will determine if the application is operated. The more complex applications developed in-house are more likely to be operated where those that are not complex which will run by themselves.

[13] The selected data base management system may need to be installed onto the computer or server for use by the entity if not already installed on the computer when purchased.

Once the external auditor understands which of the IT life cycle tasks are applicable to each component of the access path, he/she will need to understand which of the control objectives need to be addressed through the life cycles tasks of each component to identify which are relevant to the audit (3.13.2.3).

4.4.4.4. IT Governance – IT life cycle: CAVI

The external auditor clearly needs to understand the control objectives to assist him/her in identifying which controls are relevant to the audit (3.13.2.3). The external auditor will need to identify, for each relevant component of an access path, which of the control objectives being validity, accuracy, completeness and data integrity would be applicable to that component. The author has considered which control objectives would apply to the common components of the access path discussed below in Table 3.

Table 3: Components of an access path linked to relevant control objectives

Common components of an access path	Complete-ness (C)	Validity (V) [1]	Accuracy (A)	Data Integrity (I) [2]
User computer (Desktop or lap top)		X		x
Mobile device		X		x
Installed device operating software (User computer or Mobile device)		X		x
Network switch		X		x
Network router		X		x
Firewall		X		x
ADSL		X		
VPN		X		x
Internet [3]				
Server		X		x
Server operating software		X		x
Applications	X	X	x	x
Data base management system		X	x	x
Data base		X		x

Legend table 3:

[1] Validity will include the objective to prevent unauthorised access to the component of the access path, be it malicious or erroneous, as well as the risk of inappropriate segregation of duties for IT tasks associated with the access path component. This will indirectly address the requirement to protect privacy of individuals and confidentiality of organisational information.

[2] Data integrity will include the objective to prevent unauthorised access to make changes to the underlying data or processing of data on the data bases within the IT system.

[3] The internet in itself will not be within the control of the organisation. The other components of the access path, for example the firewall and router, should address the risks that arise through the use of the internet and achieve the required control objectives.

Table 3 shows that each of the components in the access path have risk exposure to at least one of the control objectives not been met. For this reason it appears, at first, as if the external auditor will need to assess if the controls surrounding each of the IT life cycle tasks for each of the components of the access paths are addressed. However, as this proposed extended approach is to be used by the external auditor in conjunction with the current general and application IT controls (4.2.1 & 4.2.2) it needs to be considered if any of the IT Life cycle tasks have already been included within the General and Application IT control risk assessment.

Certain of the tasks performed at the initial part of the IT Life cycle are already addressed in the General IT control assessment and Table 4 shows which life cycles tasks are still to be considered by the external auditor and the reason for consideration.

Table 4: Life cycle tasks of components of an access path that require additional consideration by the external auditor

Common components of an access path	Control objective(s)[2]	Hard-ware build[1]	Soft-ware build[1]	Setup or instal-lation[1]	Confi-guration	Opera-ting a com-puter	Main-tenance
User computer (desktop or lap top)	V,I						x
Mobile device	V,I						x
Installed computer (desktop or lap top) operating software	V,I				x	x	x
Installed mobile device operating software	V,I				x		x
Managed Network switch	V,I				x		x
Unmanaged Network switch	V,I						
Network router	V,I				x	x	x
Firewall	V,I				x	x	x
ADSL	V,I						
VPN	V,I				x		x
Server	V,I				x	x	x
Server operating software	V,I				x	x	x
Applications	C,A,V,I				x	x	x
Data base management system	A,V,I				x	x	x
Data base	V,I				x	x	x

Legend table 4:

[1] The computer hardware and software build as well as the initial set-up or installation, including the set-up parameters should have been addressed by the general IT controls. If not, these may need to be considered for individual components of the access path.

[2] Completeness (C); Validity (V), Accuracy (A) and Data Integrity (I) from Table 3.

Table 4 shows the following:

- All of the components of the access path should have been built, acquired or initially set up having gone through the entity's general IT controls that are place regarding system development and acquisition (4.2.1). There are thus no incremental risks for the external auditor to consider following the general IT control assessment.
- The control risk that needs to be addressed at this point would present itself in the form of possible changes subsequent to the initial acquisition or development of the access path component within the configuration settings, operating functions or computer maintenance that have been executed. The operating functions of the IT system may have been addressed within the general IT controls risk assessment procedures relating to the operating controls, however the external auditor needs to assess if this assessment has indeed addressed each of the relevant access path components in sufficient detail or if the assessment was conducted at a high level.
- Not all of the IT life cycle tasks are applicable to each component of the access path and would thus not require consideration by the external auditor for each access path component.
- In certain hardware components of the access path, the only consideration would be the maintenance of the access path component as the other control risks would have been addressed by the general IT controls when the component was initially acquired and set up. This is not the case with the software access path components as the software may be re-configured at a future date.

The results from Table 4 indicate that the configuration, operating and computer maintenance components of the IT life cycle will be controls that are relevant to the audit that need to be considered for several components of the access path when assessing control risk over and above the general and application IT controls prescribed by ISA 315 and supporting guidance.

In assessing the design and to a certain extent the operating effectiveness of these IT controls that have been identified as being relevant to the audit similar considerations will be made by the external auditor. These include the fact that each component of the access path will have unique audit tools built into the software for monitoring activity on the access path component that the external auditor will/should consider based on the manufacturer or developer standards and specifications. In doing so the external auditor can make use of CAAT's to extract the necessary information from the IT system. As a starting point the external auditor of the small and medium firm can consider the following general principles when assessing the relevant IT life cycle tasks:

- **Configuration:** Review the configuration settings or tables of the access path component for any changes to the configuration that have been made in the period under review subsequent to the initial set-up of the access path component. This can be performed by reviewing for example, configuration settings; activity or event logs or other audit reports that are available on or for the access path component. Consider if the change was made in line with the entity's policy and internal control requirements to ensure the control objectives are met.
- **Operating a computer:** Review the operating register for any unusual functions that were performed including disruptions to processing applications and other unusual events. Consider any incidents of unauthorised or unusual operations that have been reported to incident management during the period under review.
- **Computer maintenance**: When reviewing computer maintenance software and hardware maintenance will need to be differentiated. If software; assess if the version of the software program is the correct version, per the IT librarian register of programs and that all the necessary maintenance to the software program has been executed including software updates. If hardware; inspect the hardware has been physically maintained and review logs or incident reports related to the hardware component.

4.5. Summary overview of the comprehensive approach to support IT related control risk assessment

Using the proposed comprehensive approach, depicted in the third section of Figure 1, giving consideration to each element of IT Governance, in conjunction with the current general and application IT control assessment, will enable the external auditor of the small and medium firm, to address the strategic as well as the operational and technology level IT related control risks present at the auditee.

A summary of the research findings and the recommended approach is as follows. The external auditor of the small and medium firm, will first assess the general and application IT controls as required by the ISA, where after:

1. Understand the auditee's business imperatives in order to identify what the critical areas of importance are for their continued success.
2. Understand and map out the IT architecture that management has implemented to achieve the business imperatives, thereby ensuring IT alignment.

3. Identify each of the components of the access path's that relate the IT architectures that have been implemented to achieve the business imperatives as well as the access paths that are used to access the financial application and supporting data bases, if not already assessed in the general and application IT controls.
4. For each access path component, assess whether the component has key IT internal controls that are relevant to the audit by:
   4.1. assessing which of the IT life cycle tasks are relevant to that access path component; and
   4.2. assessing which internal control objective(s) will be achieved by appropriately implementing internal controls around each applicable life cycle task.
5. Test the design of the key controls that should have been implemented within each of the relevant IT life cycle tasks.
6. Performing test of controls to see if the internal controls that management have designed around each of the IT life cycle tasks have been implemented appropriately by using the audit tools, logs and registers *et cetera* relevant to the access path component.
7. Using the results of the test of key IT controls at a strategic and operational level (including the general and application IT controls) the external auditor can assess if reliance can be placed on the internal controls and control risk.
8. Finally using this assessment of control risk the external auditor will be able to determine the level of detection risk that he/she is willing to accept and set the audit strategy for further audit procedures.

CHAPTER 5: CONCLUSION

IT has a significant impact on every area of life and business and the rapid advances in the underlying technologies and their uses have impacted on how all areas of businesses operate including sales and marketing, products and delivery, finance and operations and vision and strategy. The leadership of modern businesses are required to govern the impact that IT has on the entity, within their business governance structure, at a strategic as well as an operational level to dispel their corporate governance responsibilities in terms of South African corporate law and King III. One of leadership's corporate governance responsibilities relate to IT governance which falls within the scope of corporate governance and is based on a set of principles included in King III. In governing the business as well as IT, the leadership of organisations supplement the principles in King III with internal control frameworks, for manual as well as IT related internal controls, to enable the leadership of an entity to demonstrate that they have adhered to required principles of King III. One of the most important frameworks that leadership of the entity needs to select and implement is a framework of internal control to manage risk, support efficiency and effectiveness of operations, compliance with laws and regulations and produce reliable financial reporting (COSO, 2013). In support of this internal control framework management selects and implements a specialised IT governance framework to enable them to effectively govern IT.

Corporate governance principles in King III acknowledge the role that combined assurance plays in providing stakeholders with comfort that leadership and management of an entity have implemented sound corporate governance principles, including those related to IT governance in running the business. External audit specifically provides independent assurance, as an element of combined assurance, that leadership and management have reported a true and fair reflection of the financial performance and financial position of the entity in the annual financial statements. Part of the external auditors consideration in providing assurance on the annual financial statements is to consider the internal control frameworks implemented by the auditee that have an impact on the information included in the annual financial statements. As IT has impacted the manner in which business is conducted and how the auditee records, processes and stores transactional and other pertinent data, IT will have impacted the manner in which an external audit is conducted as well as the focus areas when performing the external audit. The majority of audit firms in South Africa are in the small and medium categories and may not have access to in-house developed IT frameworks to apply to auditees that the larger firms do, which means that there may be IT related risks that they are not addressing in the performance of the external audit and may lead to inappropriate risk assessments.

The objective of this study was to provide the external auditor of the small and medium audit firm, with a comprehensive approach to address the impact that evolving IT and specialised IT governance internal control frameworks has on auditees.

The study commenced with a literature review that described several key concepts including, *inter alia*, the IT evolution, the governance of IT, the objective and process applied to an external audit and how IT has impacted each of the four stages of the audit process. The study showed that IT has impacted each of the four stages of the audit process. The most significant impact in the audit process identified is in understanding the entity and its environment in the planning phase of the audit followed by the consideration of IT as a Key Audit Matter in the reporting phase of the audit process. In the planning phase of the audit, the ISA have been enhanced to include specific requirements on the consideration of the IT system and the related internal controls that have been implemented by the auditee; this was the focus area of this study. The ISA include an overview of the risks, advantages, considerations and internal controls regarding IT that an external auditor should consider in the performance of the audit. However, the ISA alone do not sufficiently equip the external auditor of the small and medium firm, to identify and appropriately respond to the all of the significant risks that arise from the evolving nature of IT and how management governs IT within the auditee. Over time audit experts have added guidance to the ISA through breaking down the general and application IT controls into key control areas that the external auditor needs to consider (Marx *et al*., 2014; Von Wielligh *et al*., 2014; Boynton & Raymond, 2006; Arens & Loebbecke, 1980).

In assessing if the ISA, together with the supporting guidance, addresses the evolution in IT and the specialised frameworks used by management to govern IT the study first considered which frameworks are being used by management to govern IT. The investigation showed that management has access to several specialised frameworks to govern IT. The author selected the control areas that are included in the "*Integrated Framework*" identified by Goosen and Rudman (2013) as the basis for the assessment as it combines the control areas of three globally recognised, specialised IT control frameworks generally adopted by companies when governing IT, including COBIT, ITIL and ISO 27001 & ISO 27002.

The control areas identified by Goosen and Rudman (2013) where compared to the control areas that were identified in ISA, together with the supporting guidance, which identified control areas, at technology level, that external auditor is not addressing when solely applying the ISA in execution of the audit. This identified the need to create a comprehensive approach that the external auditor of the small and medium, firm can apply to address the risks and related controls relating to IT.

In developing the comprehensive approach (presented in third section of Figure 1) the study showed that by applying the same approach that the external auditor is currently using to assess control risk to IT within the auditee, and not solely assessing the general and application IT controls, the external auditor will address the IT related control risks. The current approach to assess control risk is presented in the first and second section of Figure 1 and includes understanding the entity and its control environment, identifying internal controls that will achieve the control objectives, which are considered key controls, and testing the design and operating effectiveness of those key controls before making a final assessment of control risk. In order to apply the current approach to assess control risk of an auditee as a result of the impact of IT, represented in the third section of Figure 1, the study found that in understanding the entity and its environment a link can be made between the elements of COSO, that the external auditor is using to understand the entity and its control environment, and the elements of IT governance. This link was made through the use of business governance and its IT governance counterpart as proposed by Boshoff (2014). Considering these elements of IT governance once again confirmed that by only considering the general and application IT controls the external auditor of the small and medium firm, is not addressing the key IT related controls that are relevant to the audit. Once the external auditor has understood each of the elements of IT governance, the control objectives are used to identify the key IT related controls that are relevant to the audit at a strategic level, including the general IT controls and strategic alignment, and at an operational level, including application and technology IT controls. Finally the external auditor will test the design and operating effectiveness of these key controls in order to determine if reliance can be placed on them when assessing control risk.

Using the comprehensive approach, in the third section of Figure 1, shows that key IT related internal controls that may be relevant to the audit include the general and application IT controls that are already being considered by the external auditor, as well as business imperatives at a strategic level and an increased number of hardware and software IT components and the related IT lifecycle tasks at an operational level. As the first finding of this study showed that the external auditor of the small and medium firm, requires additional guidance regarding IT related internal controls at a technology level the comprehensive approach was applied to examples of IT hardware and IT software components that are commonly used in IT architectures. This confirmed that testing technology level IT controls are specialised and can be complex which presented the opportunity for further research.

Further research can be conducted by expanding the list of IT hardware and IT software components in the access path that can be included in the IT architecture of companies into the comprehensive approach. Further research can additionally be conducted on developing detailed test of controls that can be performed on manufacturer specific access path components and the potential use of this comprehensive framework by the internal audit function.

REFERENCES

Aerts, A.T.M., Goossenaerts, J.B.M. Hammer, D.K. & Wortmann, J. C. 2004. Architectures in context: on the evolution of business, application software, and ICT platform architectures. *Information & Management*, 41(6):781–794.

Arens, A.A. & Loebbecke, J.K. 1980. *Auditing an Integrated Approach, Second edition*. Edglewood Cliffs, N.J.: Prentice-Hall, Inc.

Baden-Fuller, C. & Morgan, M.S. 2010. Business Models as Models. *Long Range Planning*, 43(2-3):156-171.

Beal, V. 2016a. 'ADSL'. *Webopedia.com.* [Electronic]. Available: http://www.webopedia.com/TERM/A/ADSL.html [2016, June 6].

Beal, V. 2016b. 'digital'. *Webopedia.com.* [Electronic]. Available: http://www.webopedia.com/TERM/D/digital.html [2015, August 26].

Boshoff, W.H. 1990. A path context model for computer security phenomena in potentially non-secure environments. Unpublished doctoral dissertation. Johannesburg: University of Johannesburg.

Boshoff, W.H. 2014. Masters in Accounting (Computer Auditing). Unpublished lecture slides. Stellenbosch: University of Stellenbosch.

Boynton, W.C. & Raymond, N.J. 2006. *Modern Auditing: Assurance Services, and the Integrity of Financial Reporting, Eighth edition*. United States of America: John Wiley & Sons, Inc.

Browne, J. & Zhang, J. 1999. Extended and virtual enterprises – similarities and differences. *International Journal of Agile Management Systems*, 1(1):30–36.

Bryer, R. A. 1993. The late nineteenth-century revolution in financial reporting: Accounting for the rise of investor or managerial capitalism? *Accounting, Organizations and Society*, 18(7-8):649–690.

Byrnes, P. E., Gullvist, B., Brown-liburd, H., Teeter, R., & Mcquilken, D. 2012. Evolution of Auditing: From the Traditional Approach to the Future Audit. *Aicpa*, (November), 1–9. Available: http://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/whitepaper_evolution-of-auditing.pdf [2015, November 5].

Byrnes, P. E., & Mcquilken, D. 2012. The Current State of Continuous Auditing and Continuous Monitoring. *Aicpa*, (October), 1–16. Available: http://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/whitepaper_current-state-continuous-auditing-monitoring.pdf [2015, November 5].

Center for Audit Quality. 2014. CAQ Member Alert: Cybersecurity and the External Audit. *CAQ Alert #2014-3*. Available: http://www.aicpa.org/interestareas/centerforauditquality/newsandpublications/caqalerts/2014/downloadabledocuments/caqalert_2014_03.pdf [2016, March 4].

Center for Audit Quality. 2015. Selecting Audit considerations for the 2015 Audit Cycle. *2015 Alert.* Available: http://www.thecaq.org/docs/default-source/alerts/select-auditing-considerations-for-the-2015-audit-cycle.pdf?sfvrsn=2 [2016, March 4].

Chang, S.-I., Yen, D. C., Chang, I.-C. & Jan, D. 2014. Internal control framework for a compliant ERP system. *Information & Management*, 51(2):187–205.

Christensen, B. E., Glover, S. M. & Wolfe, C. J. 2014. Do critical audit matter paragraphs in the audit report change non-professional investors' decision to invest? *Auditing: A Journal of Practice & Theory,* 33(4):71–94.

Cohen, J., Krishnamoorthy, G. & Wright, A. M. 2002. Corporate Governance and the Audit Process. *Contemporary Accounting Research*, 19(4):573–594.

Coltman, T., Tallon, P., Sharma, R. & Queiroz, M. 2015. Strategic IT alignment: twenty-five years on. *Journal of Information Technology,* 30(2):91–100.

Cordo, G.-S. & Fülöp, M.-T. 2015. Understanding audit reporting changes : introduction of Key Audit Matters. *Accounting and Management Information Systems*, 14(1):128–152.

Cragg, P. B. & Zinatelli, N. 1995. The evolution of information systems in small firms. *Information & Management*, 29(1):1–8.

Electronics glossary Whatis.com. 2005. 'digital'. [Electronic]. Available: http://whatis.techtarget.com/definition/digital [2015, August 26].

Electronics glossary Whatis.com. 2014. 'server' [Electronic]. Available: http://whatis.techtarget.com/definition/server [2016, June 2].

Emery, D. & Hilliard, R. 2009. Every Architecture Description Needs a Framework: Expressing Architecture Frameworks Using ISO/IEC 42010. *Proceedings of the 2009 Joint Working IEEE/IFIP Conference on Software Architecture and European Conference on Software Architecture (WICSA/ECSA 2009)*. 31–40.

Flesher, D. L., Previts, G. J. & Samson, W. D. 2005. Auditing in the United States: A historical perspective. *Abacus*, 41(1):21–39.

Flowerday, S., & von Solms, R. 2005. Real-time information integrity=system integrity+data integrity+continuous assurances. *Computers & Security*, 24(8):604–613.

Fraser, I. & Pong, C. 2009. The future of the external audit function. *Managerial Auditing Journal*, 24(2),104–113.

Gantz, S.D. 2014. *The basics of IT audit: purposes, processes, and practical information.* Waltham: Syngress.

Gartner. 2015. Hype Cycle for Emerging Technologies Identifies the Computing Innovations That Organizations Should Monitor. *Gartner.com.* [Web log post]. Available: http://www.gartner.com/newsroom/id/3114217 [2016, June 20].

Gerow, J.E., Thatcher, J.B. & Grover, V. 2015. Six types of IT-business strategic alignment: an investigation of the constructs and their measurement. *European Journal of Information Systems*, 24(5):465-491

Gheorghe, M. 2010. Audit Methodology for IT Governance. *Informatica Economică*. 14(1):32-42.

Goosen, R. & Rudman, R. 2013. An Integrated Framework To Implement It Governance Principles At A Strategic And Operational Level For Medium-To Large-Sized South African Businesses*. International Business & Economics Research Journal,* 12(7):835-854.

How VPN Works. 2003, March 28. *Microsoft.com.* [Web log post]. Available: https://technet.microsoft.com/en-us/library/cc779919(v=ws.10).aspx [2016, June 6].

Huang, S. M., Hung, W. H., Yen, D. C., Chang, I. C. & Jiang, D. 2011. Building the evaluation model of the IT general control for CPAs under enterprise risk management. *Decision Support Systems*, *50*(4):692–701.

Imhoff, E. A. 2003. *Accounting Quality, Auditing, and Corporate Governance (2003, January)*. Available at SSRN: http://ssrn.com/abstract=374380 or http://dx.doi.org/10.2139/ssrn.374380. [2016, September 18].

Independent Regulatory Board for Auditors (IRBA). 2016. *Annual Report 2015/2016*. Available: https://www.irba.co.za/upload/ANNUAL%20REPORT%202016%20final.pdf [2016, October 12].

Information Systems Audit and Control Association (ISACA). 2014. *COBIT 5 Process reference model – Processes for Governance of enterprise IT.* Available: http://www.isaca.org/COBIT/Documents/COBIT-5-Enabling-Processes-Laminate_res_Eng_0812.pdf [2015, October 15].

Information Systems Audit and Control Association (ISACA). 2014. *ISACA Glossary of terms.* Available: http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf [2015, March 31].

Information Systems Audit and Control Association (ISACA) & Protiviti. 2015. *A Global look at IT audit best practices. Assessing the international leaders in an annual. ISACA/Protiviti Survey.* Available: http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/a-global-look-at-it-audit-best-practices.aspx [2016, March 4].

International Organisation for Standardisation. (ISO). 2011. *ISO/IEC 42010 Systems and Software Engineering — Architectural Description.*

Institute of Directors Southern Africa (IODSA). 2009. *King Code of Governance for South Africa.*

Institute of Directors Southern Africa (IODSA). 2016. *Draft King IV Report on Corporate Governance for South Africa.*

IT Governance Institute (ITGI). 2015. [Web log post]. *Itgi.org.* Available: http://www.itgi.org/About-Governance-of-Enterprise-IT.html [2015, June 9]

Janvrin, D., Bierstaker, J. & Lowe, D.J. 2008. An Examination of Audit Information Technology Usage and Perceived Importance. *Accounting Horizons,* 22(1):1–21.

Julisch, K., Suter, C., Woitalla, T. & Zimmermann, O. 2011. Compliance by design - Bridging the chasm between auditors and IT architects. *Computers and Security*, *30*(6-7):410–426.

Kaufman, F. 1961. *Electronic Data Processing and Auditing*. New York: Ronald Press Co.

Killmeyer, J. 2006. *Information Security Architecture, an integrated approach to security in the organisation. Second edition.* Florida: Auerbach Publications.

Klann, B.K. & Watson, M.W. 2009. SOX 404 Reported Internal Control Weaknesses: A Test of COSO Framework Components and Information Technology. *Journal of Information Systems,* 23(2):1-23.

Luchetti, J.P. 2015. Why Gartner's hype cycle matters to companies and developers. *DeveloperTech.com.* [Web log post]. Available: http://www.developer-tech.com/news/2015/aug/20/why-gartners-hype-cycle-matters-companies-and-developers/ [2016, June 20].

Marx, B., van der Watt, A. & Bourne, P. 2014. *Dynamic Auditing eleventh edition.* South Africa: LexisNexis.

Matthews, D. 2006. *A history of auditing.* Oxon: Routledge.

Mutsaers, E.-J., van der Zee, H. & Giertz, H. 1998.The evolution of information technology. *Information Management & Computer Security,* 6(3):115-126.

Okoli, C. & Schabram, K. 2010. A Guide to Conducting a Systematic Literature Review of Information Systems *Research. Sprouts: Working Papers on Information Systems*, 10(26):1-49.

Op't Land, M., Proper, E., Waage, M., Cloo, J. & Steghuis, C. 2009. *Enterprise Architecture Creating Value by Informed Governance*. Heidelberg: Springer-Verlag.

Osterwalder, A. & Pigneur, Y. 2010. *Business Model Generation: A Handbook for Visionaries, Game Changers, and Challengers*. Amersterdam: Alexander Osterwalder & Yves Pigneur.

Oxford English Dictionary. 2014. 'workflow'. [Electronic]. Available:http://www.oed.com/view/Entry/400203?redirectedFrom=workflow#eid [2015, August 11].

PriceWaterhouseCoopers (PwC). 2010. *Combined Assurance. Implementing a combined assurance approach in the era of King III. Available: https://www.pwc.co.za/en/assets/pdf/steeringpoint-kingiii-combined-assurance-11.pdf [2016, June 20]*

Rai, L. P. & Lal, K. 2000. Indicators of the information revolution. *Technology in Society*, 22(2):221–235.

Republic of South Africa. 2008. *Companies Act 71 of 2008.* Available: http://www.justice.gov.za/legislation/acts/2008-071amended.pdf [2015, April 16].

Republic of South Africa. 2013. *Protection of Personal Information Act 4 of 2013. Available: http://www.justice.gov.za/legislation/acts/2013-004.pdf* [2015, April 16].

Robson, K., Humphrey, C., Khalifa, R. & Jones, J. 2007. Transforming audit technologies: Business risk audit methodologies and the audit field. *Accounting, Organizations and Society,* 32(4-5):409–438.

Rubino, M. & Vitolla, F. 2014. Internal control over financial reporting: opportunities using the COBIT framework. *Managerial Auditing Journal,* 29(8):736-771.

Salamone, S. 2002, August 27. Get IT Done: Software VPN vs hardware VPN. *TechRepublic.* [Web log post]. Available: http://www.techrepublic.com/article/get-it-done-software-vpn-vs-hardware-vpn/ [2016, June 7].

Sanker, G. 2013, May 21. What Is ITIL: A Simple Explanation. *ITSMTransition.com.* [Web log post]. Available: http://itsmtransition.com/2013/05/what-is-itil-a-simple-explanation/ [2016, June 1].

Sayana, S.A. 2002. Auditing General and Application Controls. *ISACA Journal,* 5:1-3. Available: http://www.isaca.org/Journal/archives/2002/Volume-5/Pages/Auditing-General-and-Application-Controls.aspx [2015, September 3].

Singleton, T. 2010. The Minimum IT Controls to Assess in a Financial Audit (Part I). *ISACA Journal*, 1:1–3.

Singleton, T. 2010. The Minimum IT Controls to Assess in a Financial Audit (Part II). *ISACA Journal*, 2:1–5.

South African Institute of Chartered accountants (SAICA). 2015. *Code of professional conduct of the South African Institute of Chartered Accountants.* Effective April 1, 2014.

South African Institute of Chartered accountants (SAICA). *2016. SAICA Membership Statistics: Constituencies 2016.* Available: https://www.saica.co.za/Portals/0/Members/About%20members/Constit2016.pdf [2016, October 13].

Swanepoel, E. 2013. The extent of the use of statistical sampling in the audits of listed companies. *South African Journal of Accountability and Auditing Research.* 14:1–13.

Sylvester, A., Tate, M. & Johnstone, D. 2013. Beyond synthesis: re-presenting heterogeneous research literature. *Behaviour & Information* Technology, 32(12):1199-1215.

Teece, D.J. 2010. Business Models, Business Strategy and Innovation. *Long Range Planning*, 43(2-3):172-194.

The Committee of Sponsoring Organizations of the Treadway Commission Internal control (COSO). 2015. *COSO in the Cyber Age*. Available: http://coso.org/documents/COSO%20in%20the%20Cyber%20Age_FULL_r11.pdf [2015, June 8].

The Committee of Sponsoring Organizations of the Treadway Commission Internal control (COSO). 2013. *Internal Control - Integrated Framework Executive summary.* Available: http://www.coso.org/documents/990025p_executive_summary_final_may20_e.pdf [2015, June 8].

Tuttle, B. & Vandervelde, S. D. 2007. An empirical examination of CobiT as an internal control framework for information technology. *International Journal of Accounting Information Systems*, *8*(4):240–263.

University of Arizona. 2016. Search Strategy Builder. Available:http://www.library.arizona.edu/help/tutorials/searchBuilder.html [2016, June 28].

University of Stellenbosch. 2016. Unpublished Auditing Undergraduate and Honours Curriculum. Stellenbosch: University of Stellenbosch.

Vasarhelyi, M. A. & Romero, S. 2014. Technology in audit engagements: a case study. *Managerial Auditing Journal*, *29*(4):350–365.

Von Wielligh, S. P. J. 2006. The incorporation of actuarial expertise in overall audit strategies for listed South African long-term insurers. *Meditari Accountancy Research,* 14(2):113–130.

Von Wielligh, P., Prinsloo, P.,Penning, G., Butler, R., Nathan(Josset), D., Kunz, R., Motholo, V., O'Reilly, G., Rudman, R. & Scholtz, H. 2014. *Auditing Fundamentals in a South African context.* Southern Africa: Oxford University Press.

Webopedia. 2016. 'traffic'. [Electronic]. Available: http://www.webopedia.com/TERM/T/traffic.html [2015, August 26].

Webster, J. & Watson, R.T. 2002. Analysing the past to prepare for the future: writing a literature review. *MIS Quarterly*, *26*(2):xiii-xxiii.

Weske, M. 2010. *Business Process Management, Concepts, Languages, Architectures.* Heidelberg: Springer-Verlag.

What is a firewall?. 2016. *Microsoft.com.* [Web log post]. Available: https://www.microsoft.com/en-us/safety/pc-security/firewalls-whatis.aspx [2016, June 2].

What is a Network Switch vs. a Router?. 2016. *Cisco.com.* [Web log post]. Available: http://www.cisco.com/cisco/web/solutions/small_business/resource_center/articles/connect_employees_and_offices/what_is_a_network_switch/index.html?referring_site=smartnavRD [2016, June 1].

Yang Liming Guan, D. C. 2004. The evolution of IT auditing and internal control standards in financial statement audits: The case of the United States. *Managerial Auditing Journal,* 19(4):544–555.

International Standards on Auditing

IAASB Glossary of terms – IAASB (International Auditing and Assurance Standards Board). 2015 *Glossary of terms.* Effective December 15, 2009. Available: http://www.irba.co.za/upload/IAASB-2015-Handbook-Volume-1_0.pdf [2016, September, 18].

IAASB (International Auditing and Assurance Standards Board). 2015. *Overall objectives of the independent auditor and the conduct of an audit in accordance with International standards on auditing.* ISA200, Effective December 15, 2009. Available: http://www.irba.co.za/upload/IAASB-2015-Handbook-Volume-1_0.pdf [2016, September, 18].

IAASB (International Auditing and Assurance Standards Board). 2015. *Agreeing the terms of audit engagements.* ISA210, Effective December 15, 2009. Available: http://www.irba.co.za/upload/IAASB-2015-Handbook-Volume-1_0.pdf [2016, September, 18].

IAASB (International Auditing and Assurance Standards Board). 2015. *Identifying and assessing the risks of material misstatement through understanding the entity and its environment.* ISA315 (Revised), Effective December 15, 2013. Available: http://www.irba.co.za/upload/IAASB-2015-Handbook-Volume-1_0.pdf [2016, September, 18].

IAASB (International Auditing and Assurance Standards Board). 2015. *The auditor's responses to assessed risks.* ISA330, Effective December 15, 2009. Available: http://www.irba.co.za/upload/IAASB-2015-Handbook-Volume-1_0.pdf [2016, September, 18].

IAASB (International Auditing and Assurance Standards Board). 2015. *Audit Evidence.* ISA500, Effective December 15, 2009. Available: http://www.irba.co.za/upload/IAASB-2015-Handbook-Volume-1_0.pdf [2016, September, 18].

IAASB (International Auditing and Assurance Standards Board). 2015. *Communicating key audit matters in the independent auditor's report*. ISA701 (Revised), Effective December 15, 2016. Available: http://www.irba.co.za/upload/IAASB-2015-Handbook-Volume-1_0.pdf [2016, September, 18].

APPENDICES

Appendix 1: Mapping of the General IT controls in ISA315 to the strategic control areas identified by Goosen and Rudman (2013)

Appendix 1 assesses if the ISA, and supporting guidance, will suffice in addressing all of the risks that the evolution of IT has presented to businesses as well as the advancements in IT internal control frameworks to address those risks (4.3). To do so the General IT control areas per the ISA, and supporting guidance, were mapped to the strategic control areas identified Goosen and Rudman (2013).

General IT controls per ISA315	**General IT controls (4.2.1)** (Von Wielligh *et al*., 2014; Marx *et al*., 2014; Boynton & Raymond, 2006; Arens & Loebbecke, 1980)	**IT General control areas per Auditing Fundamentals** (Von Wielligh *et al*., 2014)	**Strategic control areas (3.7)** (Goosen & Rudman, 2013)
Oversight controls	Organisational controls and personnel practices	Responsibility levels and reporting lines.	Determine Business Policies and strategies
			Implement Business-IT alignment strategies
			Service level management procedures
			Implement Accurate IT resource management
			Financial management
			Human resource security
		Segregation of duties	Human resource security
		Staff practices	Human resource security
		Staff supervision and review	Human resource security

Appendix 1: Mapping of the General IT controls in ISA315 strategic control areas identified by Goosen and Rudman (2013) (continued)

General IT controls per ISA315	**General IT controls (4.2.1)** (Von Wielligh *et al*., 2014; Marx *et al*., 2014; Boynton & Raymond, 2006; Arens & Loebbecke, 1980)	**IT General control areas per Auditing Fundamentals** (Von Wielligh *et al*., 2014)	**Strategic control areas (3.7)** (Goosen & Rudman, 2013)
Data centre and network operations	Operating controls	Scheduling and production runs and processing	1&2
		Operating activities and use of assets	1&2
		Library controls	Business continuity management
		Business continuity controls	Problem management Business continuity management
System software acquisition, change and maintenance **Application system acquisition, development and maintenance** **Program change**	System development and acquisition controls Program change controls System maintenance	Request and needs assessment	Procurement management
			Change, release and deployment management
		Project management	Project management
		Planning and design, Development and testing, Implementation, Post implementation review.	Change, Release and deployment management
			The acquisition and development of an information system and maintenance controls
			Implementation of an information management system
			Configuration management
			Compliance requirements

Legend Appendix 1:

[1]These control areas are at an operational level, thus not addressed in the strategic control areas identified by Goosen and Rudman (2013).

[2]At an operational level these control areas will be represented within the implementation of the configuration control, specifically operate for each component in the access path.

Appendix 1: Mapping of the General IT controls in ISA315 to the strategic control areas identified by Goosen and Rudman (2013) (continued)

General IT controls per ISA315	**General IT controls (4.2.1)** (Von Wielligh et al., 2014; Marx *et al.*, 2014; Boynton & Raymond, 2006; Arens & Loebbecke, 1980)	**IT General control areas per Auditing Fundamentals** (Von Wielligh *et al.*, 2014)	**Strategic control areas (3.7)** (Goosen & Rudman, 2013)
Access security	Access controls	Security and management policy	Access controls /security management
			Risk management processes
		Physical access controls: Facilities, system, data	Access controls /security management
		Logical access controls	Access controls /security management
[3]	Business continuity controls	Operating environment: Physical dangers, Non-physical dangers	Business continuity management
		Repair and disaster recovery: Back-ups, disaster recovery plan	Problem management

Legend Appendix 1 (continued):

[3]These control areas are not specifically mentioned in ISA 315, however, as the supporting guidance suggest no IT system as a whole will function effectively without business continuity.

Appendix 2: Mapping of the Application IT controls in ISA315 to the operational or technology level control areas identified by Goosen and Rudman (2013)

Appendix 2 assesses if the ISA, and supporting guidance, will suffice in addressing all of the risks that the evolution of IT has presented on businesses as well as the advancements in IT internal control frameworks to address those risks (4.3). To do so, the Application IT control areas per the ISA, and supporting guidance, were mapped to the operational control areas identified Goosen and Rudman (2013).

Application IT controls per ISA315	**IT Application control areas (4.2.2)** (Von Wielligh *et al.*, 2014; (Marx *et al.*, 2014; Boynton & Raymond, 2006; Arens & Loebbecke, 1980)	**Operational control areas (3.7)** (Goosen & Rudman, 2013)
Application IT controls to be reviewed for individual applications identified by the external auditor to address the potential risk of significant misstatement [1]	Input controls	Access path – only the application itself Configuration controls – configure, operate & maintain
	Processing controls	Access path – only the application itself Configuration controls – configure, operate & maintain
	Output controls	Access path – only the application itself Configuration controls – configure, operate & maintain
	Master File amendments controls	Access path – only the Masterfile itself Configuration controls – configure, operate & maintain

Legend Appendix 2:

[1] The question that arises is if the applications selected for the review of the application IT controls relating to one application, generally in the financial application, in isolation will address all the IT control risks that arise from the each of the technological components of the access path(s) to that financial application.

Appendix 3: Consideration of the control areas identified by Goosen and Rudman (2103) to the elements of IT Governance

To consider if using the elements of IT Governance (Panel 2 in Table 1) will provide a comprehensive approach for management as well as the external auditor to address IT related risks Appendix 3 aligns each of the control areas identified by Goosen and Rudman (2013) to the elements of IT Governance (Boshoff, 2014).

IT Governance (4.4.3)	**Strategic and operational control areas Integrated Framework (3.7)** (Goosen & Rudman, 2013)
Business Imperatives	Determine Business Policies and strategies
Business Imperatives	Implement Business-IT alignment strategies
IT Architecture	Service level management procedures
Business Imperatives; IT Architecture	Implement Accurate IT resource management
IT Architecture	Procurement management
IT Architecture Access path IT Life cycle tasks – Configure	Access controls /security management
IT Architecture IT Life cycle – CAVI Access path IT Life cycle tasks – Build, set-up and configure	The acquisition and development of an information system and maintenance controls
[1]	Project management
IT Architecture IT Life cycle – CAVI Access path IT Life cycle tasks – Build, set-up and configure	Implementation of an information management system
[1]	Financial management
IT Architecture[2]	Risk management processes
Access path IT Life cycle tasks – Build, set-up and configure	Change, release and deployment management
[1]	Human resource security
IT Architecture	Problem management
IT Architecture; Life cycle tasks – Maintenance	Business continuity management
IT Life cycle – CAVI[3]	Compliance requirements
Access path IT Life cycle tasks – Configure[4]	Configuration management
Access path	Identify access paths
Access path IT Life cycle tasks – Build, set-up, configure, operate and Maintenance	Implement configuration controls

Appendix 3: Consideration of the control areas identified by Goosen and Rudman (2013) to the elements of IT governance

Legend Appendix 3:

[1] Monitoring of the IT investment and the return thereon in financial management, human resource security and project management are basic assumptions to the functioning IT within an organisation, as the focus IT governance *(3.4)* relates to business imperatives that will drive the organisation forward, these control areas are assumed to be operating effectively.

[2] The IT architecture will address the security plan (architecture) of the IT department and systems. The risk assessment processes regarding IT is a basic assumption to the functioning IT within an organisation, as the focus of IT governance *(3.4)* relates to business imperatives that will drive the organisation forward risk assessment is assumed to be considered and addressed by the internal controls of the organisation and the selected IT architecture.

[3] In implementing the life cycle-CAVI the control objectives will support the compliance requirements of the entity.

[4] Having a clear configuration management policy that is implemented during the development or acquisition of new IT hardware and software will ensure that all items are configured correctly upon acquisition.